CYBERCRIME PRECURSORS: TOWARDS A MODEL OF OFFENDER RESOURCES

A thesis submitted for the degree of
Doctor of Philosophy of
The Australian National University

Ki Hong (Steve) Chon

June, 2016

Declaration

This thesis is a presentation of my original research work. Wherever contributions of others are involved, every effort is made to indicate clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

I authorise Australian National University to lend this thesis to other institutions for the purpose of examination.

Student's signature:

Date: *June 28, 2016*

The work was done under the guidance of Professor Roderic Broadhurst at the Australian National University.

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

Supervisor's signature:

Date:

Abstract

This thesis applies Ekblom and Tilley's concept of offender resources to the study of criminal behaviour on the Internet. Offender predispositions are influenced by situational, that is the environmental incentives to commit crime. This thesis employs non-participation observation of online communities involved in activities linked to malicious forms of software. Actual online conversations are reproduced, providing rich ethnographic detail of activities that have taken place between 2008 and 2012 from eight discussion forums where malicious software and cases of hacking are openly discussed among actors. A purposeful sample of key frontline cybercrime responders (N=12) were interviewed about crimeware and their views of the activity observed in the discussion forums. Based on the empirical data, this thesis tests a number of criminological theories and assesses their relative compatibility with social interactions occurring in various online forum sites frequented by persons interested in the formation and use of malicious code. The thesis illustrates three conceptual frameworks of offender resources, based on different criminological theories. The first model ties 'offender resources' to the actual offender, suggesting that certain malicious software and its associated activities derive from the decisions, knowledge and abilities of the individual agent. The second model submits that 'offender resources' should be viewed more as a pathway leading to offending behaviour that must be instilled and then indoctrinated over a length of time through social interaction with other offenders. The third model emphasises the complex relationships that constitute or interconnect with 'offender resources' such as the nexus of relevant social groups and institutions in society. These include the Internet security industry, the law, and organised crime. Cybercrime is facilitated by crimeware, a specific type of computer software, and a focus on this element can help better understand how cybercrime evolves.

Table of Contents

List of Tables

List of Figures

List of Cases

List of Articles

Acknowledgements

This has been a long and fulfilling journey. As I sit here acknowledging the completion of my dissertation, I am endowed to express my special appreciation and thanks to those who have steered my path towards an unforgettable experience.

First of all, I am utmost grateful to my supervisor, Professor Roderic Broadhurst, who not only guided me, but also provided an insurmountable level of expertise, wisdom and support that simply cannot be quantified. Your patience and encouragement throughout my PhD experience has inspired me to continue my journey in pursuing academia and research as a career.

Furthermore, I am grateful to Professor Peter Grabosky who has provided an exemplary level of feedback as well as helpful direction. In addition, I thank Dr. Raymond Choo as you have taken such time and care to review my thoughts.

There are many incredible and talented people I have had the opportunity to come across through my research. Professor Veronica Taylor and Paulina Piira, thank you both kindly for the immense help and support. I thank the academics and researchers that I have briefly corresponded with, including (in alphabetical order by last name) Rob Ackland, Mohammad Bezyan, Lennon Chang, Paul Ekblom, Marcus Felson, Budi Hernawan, Robyn Holder, Tom Holt, Alice Hutchings, Michael Joyce, Robert Layton, Nima Masroori, Peter Sommer, Natasha Tusikov and Gregor Urbas. I have also had the privilege in collaborating with Dr. Mamoun Alazab who I have been honoured to work closely with on various cybercrime projects, which has helped guide this thesis.

Thank you to the Australian Research Council for funding the research. I am also grateful to the Australian National University Regulatory Institutions Network, my home for the first three years of my research and my current department, the Australian National University College of Arts & Social Sciences.

My appreciation also extends to those governmental agencies and security companies that I worked with to access valuable data that has steered the research. While I am unable to provide names due to confidentiality, please accept this acknowledgment as you were not only a source of information, your support for my research enabled me to analyse cybercrime problems based on first-hand, meaningful data; a crucial if not one of the most critical components that has directed the course of my PhD.

I am also indebted to Rebecca for her editorial comments. Your knowledge from the field of education theory has been influential in the methodology used to analyse the data. Finally, and most importantly, I thank my wonderful wife Joeun. I must express my gratitude for her continual encouragement and patience over the past years. She has been my inspiration to brave the journey of academic research. This thesis is also dedicated to Lydia, the newest addition to our family.

Chapter 1 Introduction

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity ...
>
> *~Gibson*[1]

1.1 Overview

In this thesis, I aim to contribute to criminological knowledge by aiming to explain the social causes and precursors of certain crime as they are manifested on the Internet. Indeed, are the reasons that drive crime in the online environment really different from those long explored by criminologists before the emergence of the Internet? Explanations of the causes of crime can vary. There are those that believe crime is influenced by the surroundings of an individual such as life circumstances or influence from peers. Others presume crime to arise as a failure of people to adopt mainstream rules and values labeled by the state. Explanations may be a combination of different issues at play or unique to the type of crime.

In an effort to further our knowledge on human action and social relationships on the Internet, it is essential to question traditional understandings of crime and criminal behaviour, and ideally, base it on empirical approaches. Relying on false or inaccurate assumptions can hinder our understanding of why crime takes place. Embarking on empirical research on cybercriminals and deviant populations has historically been problematic due to the difficulty of engaging with offenders in their natural environment, on the Internet. In light of this, a significant component of this study relies on data collected through the observation of offenders in the online environment.

Paramount among the factors contributing to crime are offender resources - software tools accessible online responsible for the compromise of computers, botnets and related illicit services - that facilitate criminal activity. Computer code and programs subsist on

[1] Quoted from *Neuromancer* by William Gibson (1990, p. 51).

computers, which are created through the use of computer languages. These programs function as tools that provide the critical means for offenders when engaging in online based activities such as theft, fraud and related deviant and criminal acts. Limited academic inquiry into understanding the responsibility of computer software in the commission of crime, and its role as a facilitator of crime has occurred to date, in particular its creation as a new technology, its refinement or development, its dissemination, and its wider adoption and use.

Finding related studies on this topic was a challenge when initially embarking on my PhD in early 2011. Over the course of my research, I have come across a growing number of notable studies on cybercrime, particularly in 2014 and 2015 prior to publishing this research. However, there continues to be a lack of inquiry on software as the subject matter in the field of criminology. Holt and Bossler (2014) made a similar observation of the little research that has been done on online markets relating to malicious software.

As will be discussed in subsequent chapters, evidence suggests online social interactions involve processes relevant to learning and knowledge transfer within communities based on web forum sites. Such interactions relate to software that both encourage and support cybercrime. The role of software as a cause of crime remains relatively unexplored in criminological research. Moreover, there is a lack of explanatory models that examine software and criminality together. In this thesis, I use the paradigm of software to be a resource *for* criminal activity. Simply put, software is acquired prior to the actual event of a crime that takes place. The creation, distribution and use of software linked to cybercrime are illegal in certain states, and remains to be a controversial topic. Both cybercrime scholars and practitioners may consider such actions to be *malum prohibitum*, and fewer *malum in se*, unless serious harm or damage is imposed. This research works toward developing a conceptual understanding of this offender resource concept drawing from long-established explanations of crime from the discipline of criminology.

The underlying premise is that offender resources, which are readily accessible online, plays a crucial role as a cause of crime. It may be one of the key causal factors behind the many incidents of computer intrusions, data theft and online fraud. Offender resources, as

defined in this thesis, broadly include any such activity linked to a malicious form of software that functions as a kind of "toolkit", software designed with a number of features all intended for a specific purpose. Such programs consist of various components designed to assist and carry out online crime, which some have coined *crimeware* to reflect its intended use for crime. Crimeware has also been described as a class of software designed to automate cybercrime (Holtfreter, Reisig & Pratt, 2008). In *Cybercrime: The Transformation of Crime in the Information Age,* scholars like Wall (2007) also observed this self-functioning, simplified and "mechanized" characteristic of cybercrime, in order to call attention to the transformation of cybercrime activity that occurred just prior to his book being published. Since mid 2000, an increasing number of Internet users, both cybercriminals and potential offenders alike, have been reported to use criminogenic software tools used to carry out a crime. Reports from the Internet security industry have hypothesised the increase in occurrences of Internet crime to be a consequence of the availability and access to such software (Symantec, 2010; Trend Micro, 2011; Trend Micro, 2011a; Damballa, 2011). As a potential policy implication and strategy to prevent crime, these resources may be a *pinch-point* to disrupt criminal activity and a useful point of investigation. It may perhaps be possible to reduce crime by deterring or preventing circulation of such types of software on the Internet.

Some criminologists may consider the notion of an offender resource as a peripheral and even a trivial subject. Using the example of a home burglary, an offender resource would be the tool used, such as a lock pick used by an individual to break into a house. As will be discussed in the study, resources employed, accessed and used to facilitate data theft over the Internet can be as simple as a basic tool like a lock pick but also concerns a range of different actors, social processes and technical characteristics. Furthermore, it should be noted that investigating the technical facets of software makes such a topic conceivably arcane to those unfamiliar with developing software code. The findings presented in this thesis do not discuss the technical underpinnings of *how* crimeware works, the technical configuration, rather this thesis will discuss *what* crimeware does in certain cases, the rationality of crimeware, which will be the focus of Chapter 5. Knowledge of software development or an in depth technical understanding of computers is not required to grasp the concepts discussed in this research.

Traditional empirical crime research has either focused on understanding offenders or preventing crime. Academic inquiry in relation to resources as the central topic, more specifically on activity related to software used for malevolent purposes, has predominantly taken place in the discipline of computer and information security where technical measures to protect systems and data are the principal focus. In these disciplines, the emphasis has been to reduce the opportunities for online offenders, and seldom address the causes of such behaviour and how software may adapt or evolve to facilitate criminal acts.

There are few empirical studies that explore software implicated with crime on the Internet. However, comparisons can be drawn between software and “traditional” offender resources. For example, firearms are ostensibly linked to street crimes and violence similar to how crimeware is associated with hacking. Both are seemingly adverse technologies and pervasive in today's society. Processes of criminalisation have occurred for both firearms and crimeware in certain countries raising contentious debate. For example, Germany criminalised hacking tools in 2007. On other hand, software is distinct in other ways. Software is inherently *neutral* as it does what we instruct it and what it is designed to do, essentially automated as mention previously. Software is ultimately created ex nihilo (out of thin air); it is an *intangible* and *inanimate* entity. The dilemma arises as software has unique characteristics that allow it to be replicated and commanded for any purpose, and in the case of this study, for the purposes of wrongdoing.

While the research has relevance to widespread forms of crime, there is a specific focus on opportunistic crimes that are largely associated with profit as a motivation. The individuals observed on the web forum sites can be considered to be analogous to the online version of delinquents or street criminals. Street crimes are ordinarily perpetrated by opportunistic individuals, but can also involve organised groups. The development process of crimeware in certain cases, as revealed in the study, is not a solo venture and involves communication and assistance from multiple individuals. Victims targeted are often the "low-hanging fruit" (Wall, 2008), such as targeted in common street crimes. Crime categories of interest cover online fraud and deceptive practices concerning cyber theft and damage, which in many cases involve the illegal access of computers or the theft of personal private information.

Lastly, the findings and discussion may have linkages to online crime that are ideologically motivated or possibly state-sponsored. However, such occurrences are considered different topics raising disparate questions. Increasingly reported by the media in recent years is the topic of hacking incidents as a form of online protest, which is beyond the scope of this thesis.

It is important to recognise that criminals that are arrested and prosecuted are not representative of all those that commit crime on the Internet. On the other hand, the observable offenders online are only a subset of offenders on the Internet and not all offenders are connected to crimeware activities. Furthermore, the variability of the illegality of certain acts observed in online communities that involve illicit or crime-like activity may not be illegal in view of the law in some jurisdictions, and may not be viewed as "criminal" by those participating in such communities as well as external observers. In light of the varying points of views, the notion of crime, adopted in this research, may be better described as behaviour or activity of a malicious nature, akin to the natural law understanding of crime which entails a probability of harm, regardless if directed toward a person, organisation or computer. The term offender is used loosely, in this thesis, to refer to *potential* offenders and individuals associated with crimeware activity in some form. Though the empirical data collected is not presumed to represent all cybercrime activity, the research is a step toward advancing our understanding of offender behaviour.

It will be revealed that individuals learn to become criminals through online interactions. The discussion content also indicates that web forum site members exhibit qualities of the rational criminal. The individuals that participate in web forum sites are actively learning how to deploy and operate botnets, they are acquiring knowledge on hacking techniques, actors in certain cases are openly developing crimeware tools, and it is also clear the selection of targets is deliberate based on factors such as its weakness, vulnerabilities and the technology it uses, to list a few examples. Furthermore, online crimeware communities play a role and function in society. For instance, web forum sites offer a source where individuals can learn to protect and secure systems on the Internet.

1.2 Definition of Key Concepts

Cybercrime

At present, there is no agreed upon universal definition of what constitutes cybercrime. As noted by Chang (2012), terms such as "cybercrime", "cyber crime", "computer crime", "computer-related crime", "hi-tech" crime," "technology-enabled crime", "e-crime", and "cyberspace crime" are often used interchangeably. The meaning of cybercrime is broad and may be better understood as an umbrella term encompassing a variety of activities. For example, online child exploitation, state sponsored hacking and theft of hardware is sometimes grouped under cybercrime. Such crime can also be classified based on whether a computer is an instrument, target or merely incidental to a crime (Smith, Grabosky & Urbas, 2004). Terms such as "crime", "cybercrime" and "online crime" will be used interchangeably throughout this thesis.

Delineated in the summary section of the *Convention on Cybercrime* that was drafted by the Council of Europe (COE) in 2001 along with Canada, Japan, South Africa and the US, cybercrime includes events “committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security”. The specific types of crime that can be linked to this research are pertinent to computer-related fraud and violations of network security. There is also a focus on utilitarian crimes typically associated with profit gain. The sorts of cybercrime of interest in this research, as observed in the data examined, indicate personal gain as one motivation. However, such motivation may be one of many, as motivation is complex and may include psychology orientation, social influences, and environmental and life factors. The assumption is made in this study that financial benefit, or more generally personal gain, is a chief rationale for crime, but other motivating factors are not ruled out. Motivation can change over time, and there may be different motivations depending on the circumstances and situation of the offender.

Highlighted on the Australian Federal Police (2013) website, the Computer Offences section in part 10.7 of the *Criminal Code Act 1995* (Australia) describes cybercrime as "high tech crime" which includes:

- computer intrusions (for example, malicious hacking)
- unauthorised modification of data, including destruction of data
- denial-of-service (DoS) attacks
- distributed denial of service (DDoS) attacks using botnets
- the creation and distribution of malicious software (for example, viruses, worms, trojans)

In this research, the definition as outlined in the Australian *Criminal Code Act* is adopted. With regards to this definition, it is important to note that, in many cases, activities are often interconnected. For example, the source of many distributed denial of service[2] (DDoS) attacks is widely understood to originate from botnets: networks of compromised computers controlled by cybercriminals. Computers initially become compromised through the intentional act of hacking by actors, which is an example of computer intrusion. Hacking implicitly entails the task of modifying, destroying or the covert downloading of data, unknown to the computer's owner. These events can occur through the use of crimeware available for download from third parties. These various scenarios are seemingly linked and may not occur in isolation.

Offender Resources

This study explores offender resources associated with online criminal activity. It is a concept that is the focus of this research and developed in subsequent chapters. A resource, in a general sense, can be any source that provides some sort of gain for a person. The offender is the person viewed to benefit, albeit likely for dishonest aims. For the purposes of this research, offender resources are defined as the *availability* of factors - potentially attainable if not already accessible - that influence or enable individuals when engaging in law-breaking or delinquent behaviour.

[2] *Distributed denial of service* (DDoS) is an attack by malicious actors to temporarily make unavailable a computer or website connected to the Internet. The attack involves over burdening the target computer or website with traffic from numerous locations.

Ekblom (n.d.) views resources as *co-defined* with criminal opportunity. For example, an ATM credit card skimmer that fits over the existing reader records a personal identification number (PIN) when a customer inserts their card to withdraw money. This device is deliberately designed to look as if it is a part of the machine. The opportunity for ATM fraud is certainly only possible for criminals with the skill and capability to build such nefarious contraptions or the knowledge of where to acquire them. In other words, the resources utilised in this example are specific to achieve this criminal act. While offender resources may be determined by opportunity in many cases, the presence of applicable technology as well as the resistance to stop such crime (by individuals and organisations with objectives to stop or prevent such crime) can impact and redefine offender resources. In this thesis, a broader view is adopted in which offender resources can also be *external* to the crime and deviates from Ekblom's idea that resources must always be connected to the opportunity. Therefore, there may not be an explicit link between offender resources to the instances of cybercrime in every case presented in this thesis.

Types of offender resources broadly include technology, knowledge as well as other individuals online that interact with the offender. The role of offender resources can play either a central or secondary function in a crime, however a crime does not need to have taken place to be classified as an offender resource. The notion of an offender resource appears very similar to that of a crime facilitator. However, an offender resource implies a source that may be in abundant, or short, supply to the offender, while a facilitator operates as a means to assist the crime process. Clarke (1997) pointed out that there are "things such as automobiles, credit cards and weapons … [which] comprise the essential tools for … crime" (p. 12). Alternatively, offender resources could be viewed as facilitators that do more then simply abet crime but are also *designed* to specifically enable criminal activity, or cybercrime that is the focus here.

The relationship between crime-related resources and offenders was first put forth and discussed at length by crime scholars Ekblom and Tilley (2000), which was centered around the criminological debate on how to connect the sub-field of criminology known as

situational crime prevention[3] to offender-focused explanations of crime. A significant part of this research ventures to expand upon the notion of the "resourceful offender" that was originally introduced. Drawing from Ekblom and Tilley's concept, the underlying premise, in this thesis, draws from modern rational choice and neo-classical criminological theories that presume criminal activities follow opportunity (Newman & Clarke, 2013).

The topic of offender resources may appear as an undisputed component for their role in a crime. Cohen and Felson (1979) described crime occurring when a *likely* offender, which they state to consist of ability as well as intent (p. 590) as required for the successful execution of a crime by the offender. However, the crux of the offender resource concept is based on the line of reasoning that an offender alone is unlikely to, or possibly incapable of, committing a crime *without* assistive tools. Offenders surely have varying levels of ability, whether that includes being proficient or more generally being able to commit crime, but in the cybercrime scenario it is offender resources that provide the facility to perform the crime. Offender resources, accessed by the offender, conceivably influences *ableness* as it functions as a necessity to perform a crime. With offender resources within reach to a motivated offender, the possibility of a person to participate in widespread attacks and criminal activity increases. Likewise, the unavailability of offender resources can reduce the chances of certain crimes to happen.

Revisiting the home burglary analogy, offenders may learn that certain houses lack a security system and are thus vulnerable. Similarly, cybercriminals are known to exploit vulnerabilities of computers and servers connected to the Internet. This knowledge, details relating to vulnerabilities, is a type of resource that is acquired from some place. A resource can also include individuals such as co-offenders, in the same way peers on the Internet sometimes coordinate online hacking activities. Resources can also include intermediaries,

[3] *Situational Crime Prevention* is a sub-field of criminology that aims to make the opportunities for crime more difficult for the offender (Clarke, 1995). To provide a basic example, a strategy to reduce the chances of crime such as a home break-in would be to ensure all windows are locked and that the house has a security system. Cornish and Clarke (2003) propose 25 techniques that comprise five pillars namely, *increase the risks*, *reduce the rewards*, *reduce provocations* and *remove excuses*. Each pillar is further broken down to five techniques. The full matrix of 25 techniques can be accessed at http://www.popcenter.org/25techniques/ (Center for Problem-Oriented Policing, n.d.).

or services, with the online equivalent being the sale of stolen credit card data to a fence. A sophisticated burglar uses lock-picking devices to open a locked entrance. Correspondingly, a pseudo "cyber" lock picking device used by offenders include exploits, snippets of code that take advantage of a weakness in a system with the intention of gaining unauthorised access. In many ways cybercrime is not so different from non-Internet crimes. Nonetheless, a common theme does exist among the various sorts of offender resources in the domain of cybercrime. It is the presence of crimeware that significantly increases the opportunities for crime to happen.

From Software to Crimeware

No one would argue how integral technology and computers have become in our lives. We rely on technology to make our lives more productive, and this occurs through the help of software. Unfortunately, software can also be used for disreputable reasons such as to steal data, disrupt and destroy systems, all of which have become more common in recent years.

At its most basic level, software is a computer program that consists of a collection of instructions that enable a computer to perform some action that we direct it to do. When used by criminals, it can be explicitly instructed to perform a malicious act, that is, malicious in the view of potential victims. *Zeus*[4] is an example of software designed specifically for crime, which will be referred to and investigated in subsequent chapters. In other cases, software may be justifiable in its benefits. One such example is *Nmap*,[5] a tool that cybercriminals are likely to employ to illicitly hack into networks, which are also used by legitimate computer security professionals to ensure systems are kept secure. The *malicious attributes* of a software program do not necessarily dictate if it will be used for crime. However, it is definite that some software is created with the *intended function* to commit online fraud, as in the case of *Zeus*.

[4] Widely prevalent from 2009 to 2011, *Zeus* is a software tool with the function to steal data from a victim's computers connected to the Internet. It has also been referred to as a bank trojan as it has features designed to steal login credentials of victim's when banking online.
[5] *Nmap* is a tool that probes a computer network, which has the implicit function of revealing "holes" in a network that could potentially be breached.

To avoid ambiguity, I outline the software that is the focal point of this thesis. Malware, a portmanteau combining "malicious" and "software", has been widely used to signify software with the intended function to damage or perform unwanted acts on a computer. Similar terms, like crimeware, refer to programs with the intended function to commit crime. In this thesis, the United Nations Interregional Crime and Justice Research Institute (UNICRI) definition is used, which points out that crimeware does not function autonomously and that an individual, whether the creator or user, is responsible for its operation. UNICRI (2013) defines crimeware as:

> ... software that is utilized by an individual to commit cybercrime. It is not a program that involuntarily enables crime ... but one that deliberately enables the commission of an offence, such as keystroke loggers, backdoor programs, bots, spyware and Trojan horses ...
> (UNICRI, Crimeware, para. 1)

In the *Comprehensive Study on Cybercrime* from 2013 by the United Nations Office on Drugs and Crime (UNODC), a reference is made to *computer misuse tools* to refer broadly to computers, proxies and botnets,[6] which could also describe crimeware. The botnet infrastructure in itself could also be considered a figurative tool, and an offender resource, as it is functions as an instrument used by cybercriminals to propagate online malicious activities. As will be revealed in this study, botnets are commonly created through the employment of crimeware. Do-it-yourself (DIY) malware (Ollman, 2009) is another term referred to in reports from security companies highlighting its simplicity and ease of use. Many examples of crimeware exhibit this characteristic.

1.3 The Research Problem

Focusing on crimeware as a cause of crime

[6] A *botnet* is a series of computers connected to the Internet that is covertly controlled by malicious actors, unknown to the owner's of the computers. Data can be stolen from computers. It can also be used as a proxy to launch further activity such as transmitting spam, a platform for DDoS attacks and to perpetrate other cybercrime activity.

Cybercrime has been highlighted as opportunistic incidents by criminals and linked to the growing sophistication and evolution of malware. Crime perpetrated through automated software tools was a common theme among businesses that were victimised in Australia (CERT Australia, 2012). Although it is generally accepted to be a source of cybercrime, to date there has been little empirical inquiry on topics that intersect crime and software, apart from a few key notable studies that will be discussed in Chapter 2. Studying cybercrime by centralising the investigation on crimeware offers a path to explore one of the reasons why cybercrime occurs.

As the primary researcher of this study, I digress to acknowledge my past interest in the hacking subculture in my youth. After a 20-year hiatus, once an onlooker of an earlier form of the communities of which this thesis examines, I was surprised to see how simple it has become to engage in cybercrime. The online communities involved with crimeware, hacking and cybercrime activities can be seen as a "creeping normality", a term Jared Diamond (1995) coined to describe significant transformations in society being overlooked if it happens gradually. Anecdotal reports of high profile cyber attacks have also obscured public perceptions of cybercrime (Wall, 2008), including among the academic research community. The numerous reports on cybercrime by different organisations have provided a distorted picture due to inaccurate and erroneous reporting. In certain circumstances, exaggerating the dangers on the Internet has been deliberate, particularly in cases where there is a benefit from over-reporting, or over-exaggerating, the cybercrime problem (Andersen et al., 2013). The now common and ubiquitous activity of online communities occupied with the propagation of software used for ill intentions requires further inquiry that must be both independent and systematic.

Reports of occurrences of cybercrime from known publicised cases, investigations by law enforcement and criminal prosecutions provide some insight into the motivation and background of a range of offenders. However, very little is known about the processes, social dynamics and means of access to various resources by offenders leading up to a cybercrime. Investigating web forum sites where such software is exchanged provides insight into the precursors of cybercrime.

Building on a theoretical framework

To stress its importance, Ekblom and Tilley (2000) drew attention to the significance resources can play in the offending process and criminal opportunity. In their explanation, an offender would need to be properly resourced, or supplied with the necessary means, in order to realise a crime. Largely based on the routine activity theory of Cohen and Felson (1979), which states crimes are ultimately committed when the opportunity arises, the resourceful offender would also need to have the ability, know-how and tools to carry out a crime successfully. In some situations, collaboration with co-offenders is necessary. The basic tenet of the theory establishes that a crime occurs, or is very likely to happen, when a motivated offender (in addition to being "adequately resourced" according to Ekblom and Tilley) and a potential victim converge in the same area at the same time. Based on the view of offenders as rational thinking and hedonistic individuals, perpetrators are viewed as opportunistic deciding whether to engage in a crime by weighing-up the rewards and risks. This describes offenders that in happenstance who may simply seize the opportunities that are present. Other offenders, traditionally associated with organised crime, are more measured in devising or discovering new opportunities that require the exertion of effort or thoughtful planning. In such a case, opportunity is created where it did not exist previously. In either case it is therefore plausible that certain resources can potentially play a role in whether a crime is to occur and succeed. It will be later revealed in the findings of the research that convergence alone is insufficient to explain why cybercrime occurs, a key result with direct implications for crime prevention.[7]

Subsequent chapters will show that certain automated cybercrime activities are reliant on specific knowledge, tools and access to co-offenders, all of which are openly accessible on web forum sites that focus on crimeware, hacking and botnet activities. It will be shown that offender resources not only contribute to cybercrime activity, but also play a functionary part in the cybercrime ecosystem[8] that encompasses offenders as well as other

[7] Crime prevention strategies, including its challenges and unintended consequences, are covered in Chapter 6.5 and throughout Chapter 7.

[8] The idea of a *cybercrime ecosystem* will be covered in Chapter 6. Cybercrime can be viewed more than simply as a one-sided "problem" caused by cybercriminals. Cybercrime is also a complex

stakeholders. Focusing on the concept of offender resources by examining real online interactions on web forum sites will provide a unique viewpoint of cybercrime that is currently absent in criminological research.

This thesis builds on Ekblom and Tilley's work by advancing the concept of offender resources in cases of cybercrime. A single explanatory theory from criminology that addresses the cross-disciplinary complexities needed to understand offender resources may be lacking. However, traditional criminological theories may provide some explanatory power. Crime is multifaceted and its causes are unlikely to be explained by a single theory. Certainly, a single theory cannot adequately explain all crime, but a selection of several theories can provide valuable insight. Routine activity theory has been suggested to be useful as a *framework* to connect a range of criminological theories (Cohen & Felson, 2003). Additionally, criminological theories can be linked which share basic assumptions (Hirschi, 1986, p. 117). In this study, routine activity theory is used as a *starting point* to tie in other criminological theories of relevance. Though Ekblom and Tilley are the first to place emphasis on exploring the theoretical significance of the offender concept, it was Cohen and Felson (1979) that originally recognised the role of offender's abilities in their routine activity theory as they refer to the use of tools and appropriate skills that make possible for the offender to engage in crime (p. 591). Cohen and Felson (1979) address the presence of, "… facilities, tools or weapons … [that] influence the commission or avoidance of illegal acts" (p. 591), but where these elements situate within the routine activity theory is uncertain. Such a concept may be an element found in the environment, closely bound to the *motivated offender*, or a combination of both.[9]

This thesis aims to appraise the validity of various theories, but does not attempt to test theories per se. A modified version of the routine activity theory is proposed which allows for other theories to be considered, with offender resources as an additional requisite for a

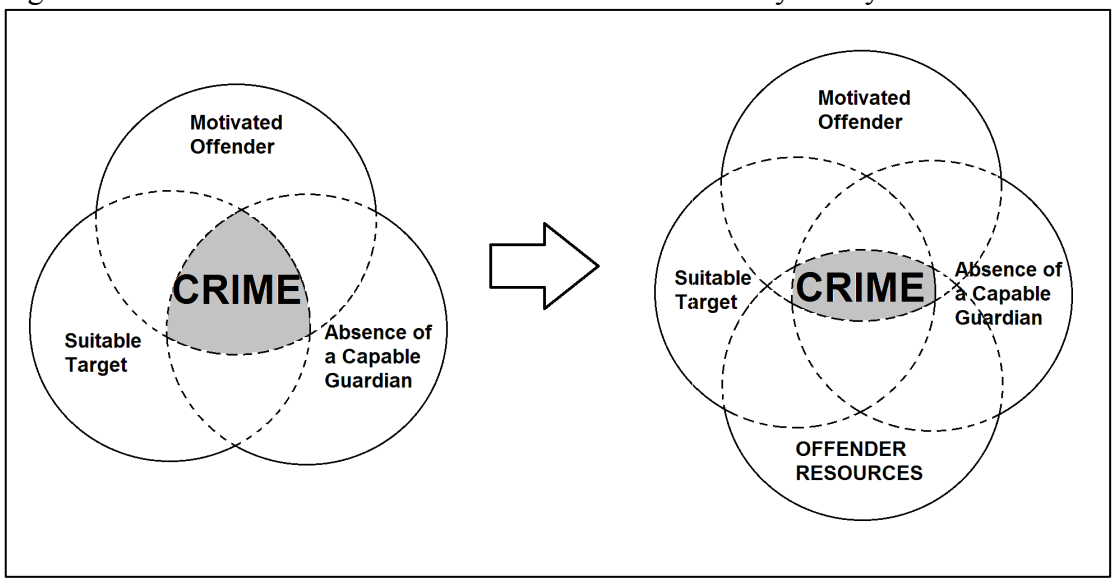
---

system that is continually changing made up of different parts. These parts, or sub-systems, can include institutions, private companies and policy.

[9] The Conjunction of Criminal Opportunity (CCO) is a framework that takes into account offender resources as a preceding factor prior to the actual event of a crime. CCO will be introduced in Chapter 2.8.

crime to occur (see Figure 1 where "offender resources" is visually depicted as a separate element to highlight its significance). This model will be revisited in Chapter 7.

Figure 1: Offender resources in relation to the routine activity theory



The first part involves examining offender resources at the micro-social level, that is, the social interactions between individuals and the role of online social association and learning in influencing crime-like behaviour. The second part focuses on the rational element of online interactions and what can be inferred from the design of crimeware and its associated activities as observed on the web forum sites. The third part of this research focuses broadly on the macro level picture such as conflicts with society about the uses of law, perceptions of the law in relation to crimeware, and offender resources as social systems of use to society.

Research questions

(1) What are the online social dynamics and behaviours among offenders?
(2) To what extent can offender interactions be explained as rationally driven processes?
(3) Where do online offender communities fit in the wider social order?
(4) How do the selected theories in the study interconnect to explain the online behaviours examined?
(5) What is a feasible theoretical model that describes offender resources?

The empirical research is primarily grounded on an online-based non-participant observation study. It also supported by data from interviews with Internet first responders and electronic data relevant to crimeware.

1.4 Summary of Chapters

Chapter 2 provides an introduction to cybercrime, highlights past relevant research and explains the theories from criminology that will be explored in subsequent chapters.

Chapter 3 outlines the methodology and data sources used to answer the research questions.

The findings are contained in Chapter 4, 5, and 6, the core chapters.

Chapter 4 investigates the social associations among offenders. This chapter answers the question, "What are the online social dynamics and behaviours among offenders?" The social interactions occurring within the web forum sites, including social dynamics such as learning processes are investigated.

Chapter 5 focuses on offenders as rational opportunity driven individuals. This chapter answers the question, "To what extent can offender interactions be explained as rationally driven processes?" It examines rationally driven processes in relation to the development, distribution and use of crimeware.

Chapter 6 examines offender resources from a macro perspective. This chapter answers the question, "Where do online offender communities fit in the wider social order?" It also explores the data from the viewpoint of social systems as well as the functionalist tradition within criminology. This chapter will also discuss offender perceptions of legality of crimeware related activities.

The discussion and final conclusion is found in Chapter 7.

Chapter 7 proposes a theoretical framework for offender resources. It also discusses the theoretical implications of the research and future research directions.

Chapter 2: Cybercrime and Theory

> Just because we don't understand doesn't mean that the explanation doesn't exist.
>
> *~L'Engle*[10]

The purpose and contribution of the thesis was outlined in chapter 1. This chapter sets out to introduce key issues on cybercrime and crimeware, and to discuss the significance of this research. This chapter comprises two sections. The first part describes the cybercrime landscape and considers what is currently known about offenders on the Internet. The second part presents key elements of a selection of criminological perspectives on the causes of crime. The explanatory significance of these theoretical views of crime will be appraised when examining the findings of the research in subsequent chapters.

2.1 Dangers of the Internet

Cybercrime affects all areas of society from the private to the public sector, ranging from home users, small to large businesses, and government. As of 2015, the total number of Internet users worldwide is over 3.2 billion (Internet Live Stats, 2015). This statistic is likely to grow with the ubiquity of mobile technologies allowing people to access the Internet from any location. As the physicist Kuhn (1962) described scientific advances creating revolutions in society, the Internet now permeates all areas of culture and has radically altered the way we live our lives. People are ever more embracing technology due in part to the release of new technological devices and decreasing cost of computers. Communication now commonly takes place exclusively in an online environment and has changed the nature of how people interact socially on all levels.

Unfortunately, society's drive for innovation and a shift towards reliance on the Internet has also brought along with it unintended outcomes, an idea originally raised by the sociologist Merton (1936) when describing events in society where there is such a focus on the intended results that the unintended consequences are left unaddressed and sometimes

[10] Quoted from *A Wrinkle in Time* by Madeline L'Engle (2010, p. 53).

ignored. These unexpected outcomes have created risk for Internet users and has manifested in the form of crime on the Internet.

Cases of cybercrime are becoming increasingly evident worldwide occurring irrespective of geographic and political borders. It is common for cybercrime offenders to initiate attacks from one country that target those in another. The cross border nature of cybercrime is frequently exploited by cybercriminals from safe havens, and thus underlines the need for cross-national and international responses to combat cybercrime (Broadhurst & Chang, 2013). In the case of Australia, cybercrime is a growing risk across society. According to a 2012 nationwide online survey by the *Australian Institute of Criminology*, which ran the months of January to March 2012 inclusive, 95% of respondents reported being exposed to at least one case of fraud over a 12-month period (Jorna & Hutchings, 2012). Businesses in Australia were also targets of cybercriminals. As uncovered in the *2012 Cyber Crime Security Survey Report* in Australia, 17% of businesses revealed confidential information being lost or stolen, 16% experienced Internet attacks that prevented the availability of their website from being accessed by customers, and 10% were victims of fraud (CERT Australia, 2012). As only identified incidents can be reported in the case of losing confidential information, the actual statistic may be higher. Instances of cases going unreported by businesses for reasons such as fear of negative publicity and potential damage to investor confidence would not be unusual. It is plausible some statistics are underestimated and inaccurate.

There is also uncertainty of the origin of the cybercrime offenders involved in attacks targeting Australia. But as national borders offer little constraint for malicious actors when attacks occur over the Internet, perhaps *pointing fingers* at the source of such activity should be less of a concern among "communities of shared fate" (Broadhurst, 2006). Combating cybercrime is a particular challenge for countries lacking cybercrime-specific legislation and policy instruments (Broadhurst, 2006). It is considered common for countries with Internet access to be affected by the cybercrime problem at some level.

2.2 Perceptions of Cybercrime

A possible challenge to understanding cybercrime can be due to the confinement of researchers in "condensing facts from the vapour of nuance" (Stephenson, 1992, p. 56 as cited in Wall, 2007). There has been an increasing interest in cybercrime related literature. However, much of what we know about cybercrime today, especially in the public domain, is influenced to a certain extent by pop culture, highly publicised news from media and reports from Internet security companies in the private sector. Wall (2007) proposed that our understanding of cybercrime falls under various discourses. The academic discourse, one of four highlighted by Wall (2007) states the object of cybercrime inquiry to be, "criminological, socio-legal, sociological, computer science, information management, economic and/or technological *understandings of what has actually happened*" (pp. 12-13).

An example of layperson's discourse, one of the four mentioned by Wall, include popular "best-seller" books. *The Cuckoo's Egg* by Clifford Stoll (1989) reveals an entertaining and illustrative account of computer criminals that exposes cybercrime as mystifying online activities depicting a murky Internet with tales of espionage and spies. Popular literature to some extent has provided a skewed, and possibly inaccurate, picture of the wider cybercrime problem. More recently published books such as *DarkMarket: How Hackers Became the New Mafia* by Misha Glenny (2012), distinguished journalist, and *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* by Kevin Poulsen (2012), an infamous hacker reinvented as a technology columnist, are a few other examples. Such chronicles have glamorised accounts of the cybercrime underground, which may contain factual content, are essentially narrative anecdotes, and are questionable if they accurately portray more prevalent forms of cybercrime activity. Another area of cybercrime discourse consists of reports published by the Internet security industry, specifically from for-profit companies. A conflict of interest perceivably exists among Internet security "businesses" that have a vested interest in the industry of online protection and the reports they publish on cybercrime activity, as such organisations provide products and services to remediate the problem that they initially report on. One can easily debate the conflict of interest that arises when such organisations circuitously benefit.

Tracking cases of cybercrime proved to be a challenge over a decade ago when incidents of cybercrime went "... undetected and many that are detected go unreported" (Brenner &

Clarke, 2004), and this still continues to be an accurate assessment today for the same reasons. Adding to the ambiguity is dialogue on offenders that are often subject to misguided perceptions and stereotypes, likely persuaded by popular culture. In spite of this, academic discourse has offered certain knowledge on offenders. Broadhurst, Grabosky, Alazab, Bouhours and Chon (2013) observed that an array of offenders co-exist based on reported incidents, including those that match the lone offender category with examples that offenders also exist within cohesive groups and larger ephemeral social networks. In an earlier illustration of hacker communities by Jordan and Taylor (1998), loose networks of hackers were characterised as "membership fluidity" (p. 766) due to the lack of social structure and absence of formal steps to join. This earlier depiction suggests there is no formal organisation. For cybercrime involving multiple actors, Wall (2014) points out the necessity to identify a better model to describe the organisation of cybercrime, which is sometimes and incorrectly assumed to be a top-down hierarchy distinctive of the traditional mafia. Empirical inquiries on understanding the nature of offending and online social interactions that affect offending behaviour are lacking. Reported cases of solo offenders and groups are frequent but relatively little is known about the circumstances that lead such individuals to become cybercriminals. Chapter 2.3 and 2.4 will present what is currently known about offenders and their social dynamics in the online environment.

2.3 From Hackers to Cybercriminals

Commentators associate the beginnings of hacking activities and hackers as the first occurrences of cybercrime. Early accounts of hackers have often been viewed as an antecedent to what we recognise as cybercrime today. The birth of the hacker culture dates back to Massachusetts Institute of Technology (MIT) in the 1960s. Students that had been tinkering with phone switches in the Tech Model Railroad Club became interested in the MIT computer lab. In the 1984 book *Hackers: Heroes of the Computer Revolution*, one of the first references to the term "hackers" is used in which the author Steven Levy (2001) labels inquisitive students as "true hackers", individuals aiming to push the limits of technology. The term "hacker" and its associated activities were originally descriptive connoting technological exploration and ingenuity. In these very early years of the Internet, hackers were mainly involved in "... playing with systems and making them do what they

were never intended to do" (Denning, 1996), and could be better described as a hobbyist community. The origins of hacking were benign. Elements of this early hacker culture may still exist today, however cybercrime, at present, is noticeably more varied from the furtive understanding of hackers of the past.

It was not until the mid 1980s when a second wave of hackers emerged that were perceived as saboteur-like and a form of a deviant subculture (Hannemyr, 1999). Perhaps influenced by media, this second wave was often portrayed as enigmatic figures, a stereotype that is still common today when envisaging cybercriminals. The hacker culture began to take shape in the 1980s along with the formation of clubs, akin to loosely organised clubs, some of which include *Legion of Doom* (LoD) based in the US and *Chaos Computer Club* (CCC) from Germany. Groups like LoD may have been wrongly associated with criminal activity by law enforcement agencies such as the FBI, as they were never involved in any illegal activity (Sterling, 1993 as cited by Wall, 2003). In one of the earliest law enforcement cases in the US, and perhaps the first ever network “hacking” attack, the Milwaukee-based group known as the 414s was investigated for breaking into a number of high-profile computer systems (Murphy, Elmer-DiWitt, & Krance, 1983). From the mid 1980s and onward, instances of computer based criminal activity became more common and a growing concern for law enforcement and the public.

Notable empirical inquiry into understanding the psychological and social factors of offending behaviour have been carried out among academic crime scholars. Chantler (1995) published one of the earliest studies on the motivation of hackers, in which Hutchings (2013) later expanded examining the demography and life circumstances of offenders. On motivation, Chantler (1995) recognised the sensation of thrill and excitement-seeking behaviour as a reason why offenders engaged in hacking activities. Similarly, the act of hacking has also been considered as a type of social entertainment among a population of Israeli hackers (Turgeman-Goldschmidt, 2005). In the more recent study on hackers, Hutchings (2013) identified monetary gain as a common motivation for cybercriminals when engaging in cybercrime. It is uncertain if there has been a shift in the motivation of offenders between the two very different time periods in which the two studies were carried out by Chantler and Hutchings, or if the studies were based on two

different offender populations. In another seminal study, Holt (2007) interviewed offenders, as well as incorporating other sources such as web forum site data. Although the goal of Holt's study focused on how offline and online experiences relate from the view of the hacker subculture, the study has profound theoretical implications as across the 13 interviews (that took place in 2004), it was revealed that hackers had an interest and adeptness in using technology around the time of adolescence or prior to this age range. This suggests that potential offending behaviour associated with the *hacker subculture* may be engendered in the life-course of the individual and starts early on in life. The simple motivation to commit crime may just be one of multiple factors at play and other explanations should not be overlooked.

Focusing on post 2000 developments of cybercrime, Brenner (2010) identified various archetypes of frequent cybercriminals, with the key types including the *historical* hacker that hacks for "sport", which may be in decline as noted by Brenner, and, more commonly reported at present, the profit-motivated fraudster. Choo (2011) has suggested that a shift has occurred on hacking-associated cybercrime, and posits that this change has been due to the increasing sophistication of malware. It is conceivable the growth in use of malware, which also refers to *crimeware* as used in this thesis, has created new offenders, as it can function as an enabling source for cybercrime. Cybercrime is seemingly easier to commit with crimeware as intended by its design. Additionally, the demand for crimeware has spawned underground online markets where various crimeware related goods and services are disseminated.

While the reasons of offenders appear to vary, it has also been implied that the social organisation and specialisation of offenders has a role in offending behaviour (Broadhurst et al., 2013). The reason why an offender commits crime may also be a consequence of the people they interact with, that is, other offenders. Cybercrime in certain cases arises to fulfil a specific functional need for criminal skills or services, thus creating offenders with specialised roles. As previously suggested by Broadhurst et al. (2013), the offender may work alone, however interaction may be required within the larger cybercrime community if certain goods, services, knowledge, skills, tools or assistance is necessary. In the case of

online communities, web forum sites[11] and chat rooms[12] were identified by a number of researchers as settings where offenders congregate online, and will be discussed in the next section.

2.4 Social Dynamics of Cybercrime

Relevant cybercrime research that examines online communities has focused on four general areas of inquiry. The first examines online communities as underground marketplaces where illicit goods and services are exchanged. The second stream looks at the trust dynamic among offenders on web forum sites. The third draws from the interdisciplinary field of network science and focuses on quantifying the social structures of cybercrime communities. The fourth stream, less specific to online interactions, examines the learning dynamic among deviant populations.

On market-based exchanges, the first typology examines online communities on web forum sites involved in the sale of financial and credit card data. Holt and Lampke (2010) examined a selection of six web forum sites engaged in the sale of stolen credit information referred to as dumps. In the study, the market for the sale of dumps appeared to mirror legitimate markets where discounts were provided with the more dumps one purchased and, the more valuable, higher limit credit cards commanding higher prices (Holt & Lampke, 2010). Interestingly, the dumps were separated and sold according to the country location from which they originated, or were stolen, from. The observed interactions also indicated that dumps varied in price according to location, characteristics of stolen credit card details[13] and credit card limits. Moreover, the exchange of stolen financial data has been observed to take place in chat rooms. Franklin, Paxson, Perrig, and Savage (2007)

[11] *Web forum sites*, also known as Internet forums or discussion forums, is an online website that allows individuals to exchange messages typically in the form of publicly posted messages. Further details on web forums sites are provided in Chapter 3.4.

[12] *Chat rooms* are a synchronous form of text-based communication. It is a distinct form of communication where online chat occurs in real-time. Using a simple analogy, conversation over a phone would be similar to the interaction on a chat room except the exchanges are in the form of text.

[13] Characteristics that affect price include purchase limits and verification value version. CVV (credit verification value) is an encrypted value based on the card number and expiration date, which is only known by the issuing bank. It is a 3-digit number that provides an extra layer of protection. CVV2 is a slightly more secure version of CVV.

identified communication related to the sale of fraudulent financial data in chat room settings, which primarily contained advertisements for illicit goods and services, for cybercriminals, and the posting of stolen financial data such as credit numbers from Visa, MasterCard, American Express and Discover.

Studies on the social dynamics of cybercrime have focused on the economic viewpoint that concentrates on the exchange between a buyer and seller, which presume actors, are individualistic decision makers and a rational agent.[14] Generalising interactions, as mutually beneficial exchanges may be overly simplistic. Although useful to understand how an online cybercrime community operates, the nature and types of interactions are diverse and may depend on the motivation of the cybercriminal that can vary. Highlighting the different types of online actors, Zhang, Tsang, Yue, and Chau (2015) categorised members in forums, which include guru hackers, casual hackers, learning hackers and novice hackers. Certain actors may not follow this "buying and selling" paradigm.

In spite of this, activities occurring within web forum sites were not limited to illicit markets of payment card information. Holt (2013) examined ten publicly accessible Russian language web forum sites that distributed and sold various types of malicious software and attack tools. The study revealed recurring behavioural patterns among the web forum participants. In the study, three common social patterns were identified, referred to as normative orders by Holt, which include price, customer service and trust. Within the web forum sites, prices were observed to be continually questioned by potential buyers with discounts offered as way to attract customers (Holt, 2013). This sort of behaviour does not differ greatly from the market economy where buyers and sellers affect prices that are determined by supply and demand. The more valuable, better quality, goods and services necessitate higher prices, and a greater supply of any particular commodity decreases prices. This first typology examined the social interaction between online offenders as a community mainly driven by market dynamics and rationalistic actors.

[14] A *rational agent*, or actor, chooses to make decisions based on what is optimal for them, a similar assumption used in neoclassical economic theory. The rational agent, or the rational offender, will be discussed further, which will be introduced in Chapter 2.8 and expanded in Chapter 5.

The second typology examines the trust dynamic between offenders. At glance, the notion of trust in underground criminal communities may seem inconsistent as it seems illogical that a criminal could trust another. On the other hand, one could also consider the concept of trust between offenders as the absence of trust (Van Duyne, Pheijffer, Kuijl, van Dijk, & Bakker 2003) in which offenders prefer to deal with other offenders where there is the *least* absence of trust. In the study on chat rooms by Franklin et al. (2007), online markets were described as a setting initially based on distrust where reputation had to be fostered for constructive interactions between offenders to happen. As a mechanism to measure trust, labels were applied to participants such as a "verified" status. Holt and Lampke (2010) made a similar observation in which new sellers were explicitly labeled as an "unverified seller", and moderators[15] would caution buyers when dealing with a "ripper"[16], a label applied to a seller if they were found to have misrepresented their goods or services or if a buyer was dissatisfied. Such labels were used to gauge trust among online offenders in the public setting of web forum sites. It was also identified that certain offenders would circumvent the mechanisms required to establish trust. Franklin et al. (2007) observed that some members could artificially *inflate* votes, which were required to obtain a verified status in the chat room setting, by creating fake users to submit votes. The established trust between criminals increases the likelihood of synergistic *crime* relationships (Nissenbaum, 2001). Findings from such investigations indicate that being perceived as trustworthy in the online communities was considered advantageous. On the prevention of crime, Webber (2014) suggested that disrupting the trust relationships among cybercriminals could be a possible approach to stop cybercrime.

Reputation, considered analogous to trust, is the judgement of an entity, such as an individual, that is based on certain characteristics of the entity. Décary-Hétu and Dupont (2012) attempted to quantify reputation using statistical methods. In their study, it was revealed that there was a relationship between specific attributes of web forum site members and their perceived reputation. Testing the hypothesis that reputation depends on the online attributes of an actor, Décary-Hétu and Dupont identified that forum members

[15] *Moderators* act as arbitrators that control a web forum site or chat room. Their primary function is to ensure a forum or chat room function as intended. Moderators are explicitly appointed their role and are clearly labeled.
[16] *Ripper* denotes an actor that has stolen or "ripped off" another person.

preferred to deal with members with longer histories and a high number of message posts, effectively members that were more active. Such web forum site participants conceivably appeared more reliable by other members. Reputation "points" could be earned and given out between members. Other mechanisms to ensure trust, essentially to establish reputation, between members have also been identified. For example in the study by Holt (2013), a validation service, through a third party escrow-type exchange, was provided to members to check if products were in fact genuine. A third party would release funds only after the good or service provided by the seller was confirmed to be authentic. The findings of the study support that online reputation played a role in subsequent interactions. Members preferred to engage with other members with greater *positive* reputation.

The third typology looks at the networks of interactions using techniques from the discipline of network science. Highlighting the usefulness of social networking data, Holt, Strumsky, Smirnova and Kilger (2012) provided a picture of the social structure of hackers through the examination of 336 social networking site members (collected from a single Russian social networking platform called *LiveJournal*). It was recognised that hackers with substantially more social "friend" links had greater influence to proliferate cybercrime as such members are better positioned to distribute malicious software tools to those conceivably less adept at engaging in cybercrime. Yip, Shadbolt and Webber (2012) measured the network typology of private messages[17] between members from five different web forum sites. Private messages between members is another channel of communication, in addition to the public discussion posts on web forum sites that were the focus of the studies such as from Holt and Lampke (2010), Holt (2013) and Décary-Hétu and Dupont (2012). In a related paper, Yip, Shadbolt, Tiropanis and Webber (2012) determined that the use of private messages by members were relatively high on one particular web forum site known as *ShadowCrew*.[18] The large number of messages exchanged suggests a likelihood of strong social ties between certain members, and perhaps organisation. It was identified that ShadowCrew had the densest network of private messages (Yip, Shadbolt, Tiropanis & Webber, 2012) compared to the other forums examined. In a similar study, Motoyama,

[17] *Private messages* are usually referred to as PMs within web forum site communities.
[18] *ShadowCrew* was a credit card fraud web forum site that was in operation between 2002 and 2004.

McCoy, Levchenko, Savage, and Voelker (2011) identified that some individuals were members of multiple web forum sites involved in credit card fraud. Social connections may also exist between web forum sites with members frequenting multiple sites. Intriguingly, Glenny (2012) revealed that rivalries existed between credit card fraud forums. Past research has shown that there are discernible social structures within web forum sites using network science approaches.

Furthermore, examining structural relationships in cybercrime research have not been limited to human actors. Chang (2012) suggested that botnets functioned as a quasi-organised crime group. Along the same lines, Van der Wagen and Pieters (2015) used a model of organised crime that is ordinarily applied to human actors to uncover the structures of botnets.

The fourth typology involves the analysis of online communities that also function as social learning environments for deviant and criminal populations. D'Ovidio, Mitman, El-Burki, and Shumar (2009) examined adult-child abuse websites involved in the exploitation of children. In the study, website features were viewed as structures to promote learning. A few of these included the availability of chat rooms, asynchronous forums (web forums), and members-only sections. These internal website structures offered settings for criminals to interact. Virtual settings and modes of interactions among offenders are not limited to web forum sites and chat rooms, and can also encompass social network sites, instant messaging services and other platforms. Among Portuguese-speaking cybercriminals in Brazil, platforms used include *Facebook*, *YouTube*, *Twitter*, *Skype* and *WhatsApp* (Merces, 2015). Holt and Bossler (2014) have also highlighted research on a myriad of deviant populations that subsist online (outside the area of hacking and cybercrime), namely sexual deviant subcultures such as pornography (DiMarco, 2003; Quinn & Forsyth, 2005), child paedophilia (Jenkins, 2001) and BDSM (Denney & Tewksbury 2013; Durkin, 2007).

Exploring whether crime is learned through association with peers involved in criminal activity has also been investigated. Based on a population of post-secondary institution students, Higgins and Makin (2004) concluded that associating with peers involved in software piracy affected students' propensity to partake in similar activity. In a previous

study, Skinner and Fream (1997) proposed that learning models could be used to understand deviant activities related to the use of computers. Of particular note, in Skinner and Fream's (1997) investigation, there was indication that those that frequented computer bulletin boards[19] were also likely to be involved in password guessing "attacks", a common technique used by cybercriminals to gain unauthorised access to a system. It is possible that such knowledge was shared on the bulletin boards. Focusing specifically on computer hacking activities, Morris and Blackburn's (2009) study on self-reported data by university students identified that social learning theories did show promise as an explanatory model. Most empirical studies that have used social learning as an explanation for cybercrime have relied on college and university student populations for data, and in certain cases youths. A study that does focus on youths under the age of 18 is that by Marcum, Higgins, Ricketts and Wolfe (2014) to investigate hacking behaviour relying on the social learning model.

Additionally, Choo (2008) stated that traditional organised cybercrime groups use the Internet to extend their criminal activities and that there were "non-traditional" organised cybercrime groups that operate solely online. However, what was overlooked was the case of "non-traditional" organised cybercrime activity that may extend to the offline world. Leukfeldt (2014) remarked that academic research has tended to focus only on the online relationships, such as those in web forum sites and chat rooms, with terrestrial relationships of cybercrime groups being disregarded. Social interaction of cybercriminals should not always be assumed to take place virtually, although specific forms of criminality on the Internet are likely to place entirely online.

2.5 A Microcosm of Cybercrime Activity

The nature and method of cybercrime has evolved since the early days of the Internet. Grabosky (2001) made the observation of cybercrime to be the same as terrestrial based crime and simply a case of *old wine in new bottles*, an observant depiction of cybercrime and still fitting over a decade later. Underscoring the capacity of the Internet to amplify

[19] A *bulletin board*, commonly known as a bulletin board system or BBS, is a virtual location where users could exchange messages, post on public message boards, chat and download software programs. Widely popular in the early 1990s, usage declined in the mid 1990s with the growth of the Internet.

activity with its vast reach, cybercrime may be more accurately described as "*an awful lot of wine* in very many, differently shaped and capacious bottles" (Jewkes & Yar, 2010, p. 3). The idea was raised at the beginning of Chapter 1 whether cybercrime differs from other forms of crime. There are elements of cybercrime that resembles non-Internet crime and, on the other hand, there are differences that make cybercrime unique.

Criminal activity on the Internet is wide-ranging and can include an assortment of offenses such as illegal interception, copyright violation, stalking, money laundering, extortion, fraud and resource theft involving the illegal use of computers (Broadhurst & Choo, 2011). A common method of automated cybercrime at present is the use of spam and malicious websites with the goal of compromising computers (Alazab, Layton, Broadhurst & Bouhours, 2013). Ostensibly the Internet has made certain crimes simpler to carry out. Identity theft is one such example in which personal information is misappropriated for crime. The Internet has made it easier to access vast amounts of personal information on individuals for the purposes of identity theft (Smith, 2010). Deception via mail fraud occurred during the Civil War era in the US which certainly occurs today in the guise of phishing[20] through emails, instant messaging and other forms of Internet communication that attempt to trick victims into revealing personal private information. In phishing attacks, emails are sent by cybercriminals with the intention to elicit information for fraud alike traditional mail fraud of the past.

There are also forms of crime that occur exclusively on the Internet. Botnets, networks of compromised computers connected to the Internet controlled by offenders, are used as a medium for further crime (Choo, 2007). Through multiple compromised computers used as intermediaries, emails can be secretly transmitted that aim to defraud recipients (Levchenko et al., 2011). Click fraud is another scheme that pays out a small amount of money when online advertising is clicked. A program is placed on a bot, a victim's computer, which covertly automates the clicking action that generates a small payout to the cybercriminal (Kshetri, 2010). Placed on many bots, or a botnet, a payout can be vastly multiplied causing

[20] *Phishing* is a deceptive technique used by criminals to steal personal private information such as login credentials and payment card information. Common vectors for phishing include emails and websites.

online advertisers to suffer large monetary losses. Furthermore, DDoS attacks are made possible through a botnet. Numerous data packets are transmitted, in concert from a botnet, with the goal of overloading and effectively shutting down a target server (Barford & Yegneswaran, 2007). A network of compromised computers, or the botnet, is in itself a case of unauthorised access of computers.

As it is evident some crimes occur solely over the Internet, there are also crimes that traverse both the virtual and terrestrial (Yar, 2005). As observed by Chabinsky (2010), the larger criminal enterprise comprises various cybercriminals with specialised functions one of which includes money mules specifically hired to visit banks to transfer proceeds from online fraud. In certain scenarios, stolen credit card details are used to order packages, by a cybercriminal, and sent to a money mule that subsequently ships the package to another destination, that is, to the money mule "herder" (Australian Institute of Criminology, 2007). There are also cases of money mules that receive bank deposits and, after withdrawing a small cut, transfers the rest of the funds to another individual in the crime ring (Stone-Gross et al., 2013). In organised online fraud operations, cybercrime activity can often extend beyond the Internet and involve “unwitting and inexperienced” (Krebs, 2012) individuals with no requirement to access the Internet or the knowledge that they were involved in any sort of illegal activity.

Cybercrime can manifest in different forms, and the pathway and means for offenders to engage in specific acts of cybercrime are diverse. Interaction between offenders can certainly take place exclusively online and so too the offender-victim engagement, however it should be underscored that cybercrime ultimately affects the “offline”, for example, banks and financial institutions, businesses, and day-to-day Internet users.

2.6 Facilitation, Precipitation and Enablement of Cybercrime

Clarke (1992) used the term “crime facilitators” to describe indispensable items for a crime to succeed. Likewise, Ekblom and Tilley (2000) noted that offenders require physical tools to carry out a crime and lists examples such as cars, guns, knives, fake IDs, ladders, mobile phones, and so on (Natarajan, Clarke, & Johnson, 1995 as cited by Ekblom & Tilley, 2000);

such devices clearly aid the crime commission process for criminals. However, certain items can have an influential effect on whether an offender engages in crime. Wortley and Mazerolle (2013) raised the idea of "crime precipitators" to account for factors in the environment of an offender that entice criminal behaviour. In certain cases, elements external to the offender can encourage or induce a response that is representative of deviant or law-breaking behaviour. In Wortley's (1998) "two-stage model", it is suggested precipitators (events preceding the crime) and opportunity (event of the crime) should be separated and follow a sequential order. The crux of Wortley's proposal is that precipitators can influence, or more explicitly are responsible for, motivation prior to opportunity factors. Wortley (1998) further collapses his concept of precipitators as prompt (environmental cues or stimuli), pressure (social), permit (justifying behaviour), and provoke (response).

Crimeware is assumed to facilitate the crime process, but can also function as a precipitator, and an idea that is explored in subsequent chapters. A few examples of crimeware include *exploit kits* that automate the infection process when a visitor visits a compromised website. Other instances of crimeware consist of *botnet kits* that simplify the control of networks of "zombie" computers and *keyloggers* that covertly steal personal private information typed into a keyboard unknowing to the computer's owner. Such software is specifically designed for the sole function to enable cybercrime.

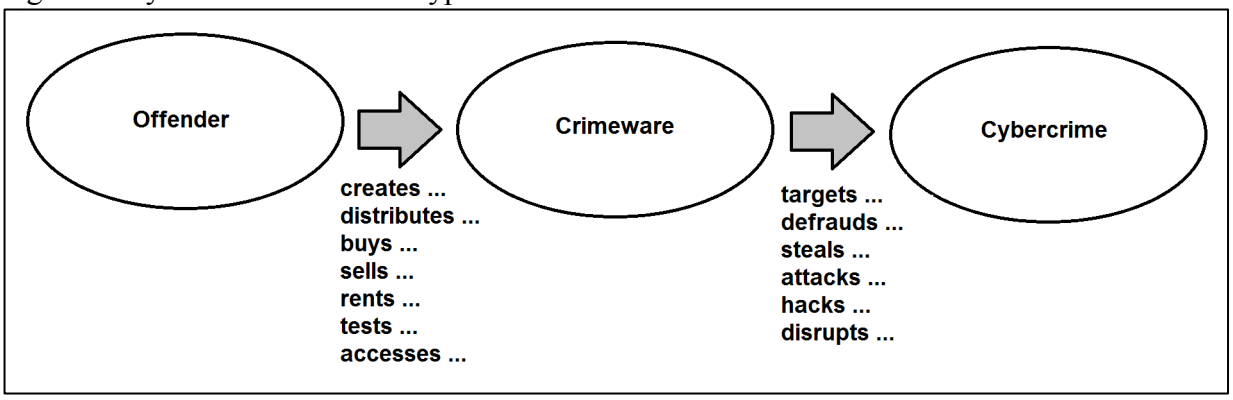
There is also software designed to "break into" websites and servers known as *penetration testing* tools, some of which are developed for legitimate use by the computer security industry. Such a category of software could be seen as a type of "criminogenic product" (Newman & Clarke, 2013), legitimate products designed for the public interest, but adapted for use in illegal activities. Crimeware in specific cases functions as a resource that contributes to the prevention of crime. For example, the *Metasploit Project* is a software platform, a product that can be purchased legitimately and widely used by legitimate Internet security professionals, which is designed to probe security vulnerabilities of computers connected over a network. Such products have been contentiously debated among Internet security professionals whether it does more harm than good as cybercriminals use the same tools (Hulme, 2012). The circulation of such *dual-use* tools paradoxically helps to protect systems and contribute to cybercrime. Perhaps such tools,

along with its operators, should be thought of as a part of an immune system (Elazari, 2014), and more specifically as an adaptive immune response. Biological cells and processes work in collaboration that are able to adapt and "train" the body to attack new viruses and germs, which resembles the affects of certain software used against systems connected to the Internet.

Yar (2005) described the *force multiplier* effect to refer to the potentially widespread activity that a single actor can cause on the Internet. Wall (2007) made the observation that automation via software would change the way in which offenders engage victims online. This amplification effect and automation characteristic of cybercrime is a relatively recent development, which have become more frequent starting mid 2000. The asymmetric and symmetric properties of the Internet (Wall, 2014) have made cybercrime, to some extent, unique compared to what one may consider being a conventional crime that occurs outside of the Internet. Multiple offenders can target a single entity in cases of hacking activities, and in other cases, a single offender can target multiple victims, for example, when botnets are used for data theft. There are broad claims in the Internet security industry that certain widespread forms of cybercrime have become prevalent due to the availability of easy to use software programs as well as an increase in botnets detected on the Internet. It is also clear offenders are availing their illicit goods and services to other offenders (Franklin et al., 2007; Yip, 2010; Holt & Lampke, 2010; Soudijn & Zegers, 2012; Décary-Hétu & Dupont, 2012; Holt, 2013) consequently facilitating various forms of online crime.

Examining the facilitation aspect of crime is fundamental in recognising how cybercrime occurs. In an actual cybercrime scenario, or the event of a crime, an offender must use or have access to a computer at some point. It is software on the computer that allows the offender to operate and instruct a computer to perform certain actions. As posited earlier, it is the use of certain categories of software, such as crimeware, that facilitate the act of cybercrime. This seemingly rudimentary, yet mandatory, step of a crime event is illustrated as a causal sequence in Figure 2 below. The premise is that crimeware must either be accessed directly, or indirectly through an intermediary, before a cybercrime can be carried out. The investigation in subsequent chapters focuses on the behaviours and activities in the crimeware stage and its surrounding social processes.

Figure 2: Cybercrime causation hypothesis



2.7 The Causes of Crime

The remainder of Chapter 2 will focus on introducing the criminological theories that will be used to examine the data in subsequent chapters. The following sections provide the theoretical "building blocks" for the purposes of developing the concept of the offender resource. The relevance of the theories as it pertains to the empirical data is presented in Chapter 4, 5 and 6. The theories discussed should be viewed as "explanatory concepts that seek to increase our understanding" (Moore, 1984), rather than an empirical exercise to confirm or refute a theory's ability to explain cybercrime.

Early inquiry into understanding crime and criminal behaviour focused on studying its causes. Classical philosophers, such as Beccaria (1764) and Bentham (1891),[21] viewed criminals as actors that fundamentally chose to break the law on their own volition. Crime was considered to be an action decided based on the free will of an individual. Park, Burgess and McKenzie (1984), on the other hand, who are better described as urban sociologists, proposed criminal behaviour was a consequence of the environment such as an individual's neighbourhood. Areas that lacked social infrastructure and economic

[21] Bentham used Beccaria's philosophy on crime to develop the idea of utilitarianism. Beccaria argued that punishment should be proportional to the crime and that the focus on punishment should be relative to harm faced by society rather than a specific victim. Bentham further expanded on the notion that the criminal was a rational individual and that the "happiness" of society should take precedence.

opportunities were believed to be more conducive environments to create criminals. Another view depicts crime as a construct created by the ruling class in society as a means to control others, as told by Marxist theorists. Different explanations have been put forth over the history of criminological inquiry with the goal to better understand the causes of crime.

Crime can also be viewed as an outcome based on a cause and effect relationship. Understanding events prior to a crime may contribute to comprehending the reasons why crime occurs. Prior events or past actions can influence an individual's or a group's current or future behaviour. To explain the cause of delinquency, Hirschi and Selvin (1967) outlined minimal standards to measure a causal relationship. To paraphrase these rules, they involve first proving a relationship exists between two events, the second component requires establishing that the relationship was not influenced by other factors, and lastly the third step entails confirming that one event did indeed occur before the other. An offender is likely to be influenced by prior events that lead them to commit crime, but determining if such events are truly a cause of crime, or merely a correlation, can be difficult if the aim is to measure causation.

Drawing from cognitive science, Cornish (1994) depicted crime as "scripts", mainly the view of crime to be made up of a sequence of steps leading up to the eventual crime. By capturing how successive events develop, Cornish envisaged that the examination of the crime commission process led to insight into the antecedents of crime, consequently helping to produce certain knowledge to help improve ways to prevent crime through the identification of intervention points. Perhaps outside the scope of its intended purpose, the proposed view of crime, at some level, connects offender behaviour (e.g., their decisions) to situational crime prevention, which has customarily been considered two disparate areas of explaining crime. Revisiting the approach laid out by Cornish, Ekblom and Gill (2015) ventured to bring to attention different ways in which crime scripts have been interpreted and applied in criminological research. Particularly relevant is the second of Ekbom and Gill's (2015) clarification of two perspectives, which emphasises the individual agent's (agents can include groups) interaction with their environment as a process that precedes

crime.[22] This process is comparable to how this thesis presents social interaction occurring within web forum sites as a precursor to cybercrime.

A selection of criminological theories will be examined when exploring the topic of crimeware as an offender resource. There are different theoretical perspectives that attempt to explain the causes of crime. Societal views of crime are generally concerned with social systems such as functionalist explanations that view crime as a part of society and integral to the proper functioning of the social order. Stemming from this functionalist view, there are also subcultural explanations in which the norms and values of mainstream society are rejected by a collection of individuals. In certain cases, this rejection can cause conflict due to divergent values between groups. Additionally, crime is also believed to be a consequence of the environment in which potential criminals *become* criminals through a process of social association. In other words, potential criminals come to be criminals if they interact with criminals. Explanations of crime are also based on the premise that crime occurs simply when the opportunity to commit a crime arises; such a view of crime explains circumstances when a crime transpires if a motivated offender in happenstance comes across a worthwhile target. Each perspective has its merits as approaches to understand criminal behaviour with some explanations having greater relevance than others when explaining cybercrime.

A semantic distinction should be clarified on the *causes of cybercrime* and the *causes of increase in cybercrime*. Cybercrime fundamentally originates due to the invention of Internet and communication technologies (ICT) - including software - and people that use them. Cybercrime could not exist without these basic elements. There are also reasons for cybercrime that have the effect of enabling or bringing about further crime. In a UNODC (2013) report, the underlying factors that explain the causes of *increases* in cybercrime are

[22] The first perspective focused on the individual agent, which include both individuals and groups. Drawing from an example by Ekblom and Gill (2015), in a hypothetical scenario person A buys a gun and subsequently goes to location B the next day to shoot person C. The second perspective is sub-divided into four components (which interestingly Ekblom and Tilley draw from observation of biological systems, specifically animal behaviour), which include function (individual behaviour influenced by the need for profit), causation (events that influence subsequent behaviour or action), development (learning or possibly the indoctrination of criminal patterns through social association) and evolutionary history.

listed (see Figure 3 below), which underscore the different paradigms of explaining the cause of cybercrime. Criminals are suggested to commit crime due to the anonymity the Internet provides (Jaishankar, 2008). As in the physical world, criminals interact online with one another and congregate to learn the skills and techniques of deviant behaviour involving the use of computers (Skinner & Fream, 1997). The convergence of cybercriminals in online communities has also revealed distinct norms and values (Holt, 2013). The social emphasis to prosper financially along with a lack of means to achieve such goals explains criminal behaviour occurring in areas with lacking economic opportunities (Bhattacharjee, 2011). Victimisation patterns have been correlated to the length of time an individual spends on the Internet, with higher Internet use increasing the chances of being targeted in phishing scams (Hutchings & Hayes, 2008). In an early seminal study on victimisation and the role of peers (specifically youths at risk of assault and robbery), it was revealed that individuals involved in certain delinquent activities were themselves more prone to becoming victims (Lauristen, Laub, & Sampson, 1992). In other words, the chance of victimisation is greater if the potential victim engages in delinquent or criminal activities compared to those that do not engage in risky behaviour. There are different explanations of the underlying causes of increases in cybercrime, each useful in different ways in advancing knowledge on offender behaviour and criminality on the Internet.

Figure 3: Underlying factors of cybercrime according to UNODC[23]

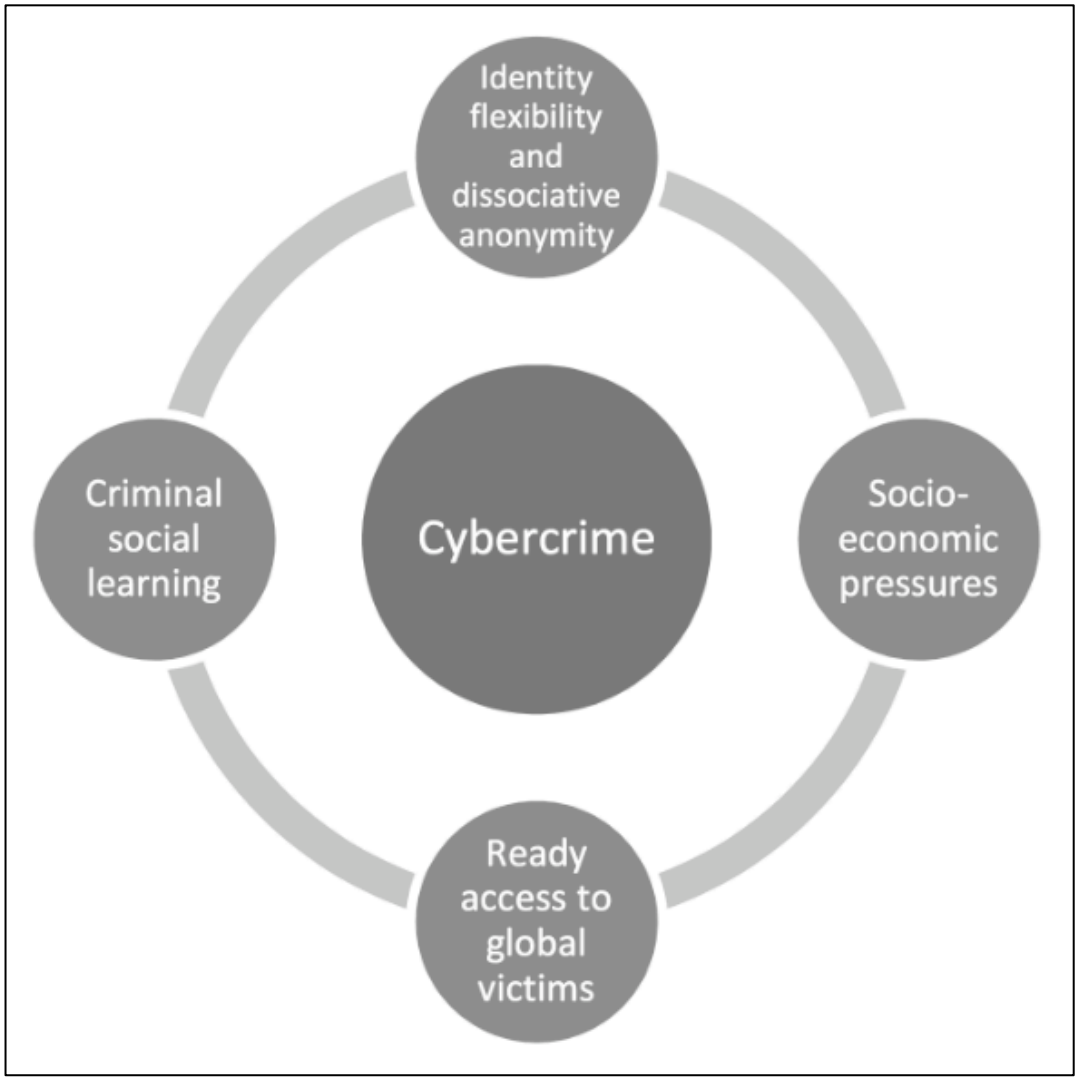


Figure 3. Possible underlying factors linked to increases in cybercrime. Copied from "Comprehensive Study on Cybercrime" (p. 8), by UNODC.

The selection of criminological theories discussed in the following sections was considered as the most applicable and supportive of offender resources as a theoretical concept in criminology. The theories derive mainly from three classical points of view from within criminology, namely the view of offenders as rational thinking actors; secondly, understanding human agency and crime through the interactions among offenders; thirdly, the macro social view that explains crime at the societal level. As presented in Chapter 1,

[23] *UNODC*, or the United Nations Office on Drugs and Crime, is the United Nations arm that endeavours to combat various forms of transnational crime, which also includes cybercrime. Its focus is primarily to provide research support, capacity building through education and promote cooperation among countries.

the routine activity theory will be used as a framework to explore the different explanations of offender behaviour connected to crimeware. The routine activity theory is predicated on the existence of the motivated offender. As postulated in the rational choice view of crime that underpins routine activity theory, such offenders consciously evaluate whether to engage in crime. The following sections introduce the three approaches starting with the view of offenders as rational actors.

2.8 Crime Follows Opportunity

The idea of criminals as individuals that freely chose to decide to commit crime was influential in the field of criminology, an idea originally established by Beccaria (1764). The free choice of offenders to commit crime was the belief that careful thought was considered to weigh out the benefits and consequences on whether to commit a crime whereby crime would likely be committed if it was worth the risk. However, if the benefits of committing a crime did not provide sufficient value to the offender at the risk of getting caught, the crime would not take place. Largely ignored for many years, Cohen and Felson (1979) re-visited the idea of criminals as individuals driven by gain and developed the routine activity theory, which is founded on the belief of the reasoning individual whose aim is to achieve their needs. Others such as Cornish and Clarke (1987) have purported to re-establish this view of offenders as actors that carry out purposive actions.

Premised on the notion of criminals as utility maximising individuals, Cohen and Felson (1979) introduced the basic tenets of routine activity theory, which established that a crime occurs, or is very likely to happen, when a motivated offender and a potential victim that is not protected converge in the same area at the same time. The assumption was that psychological and social factors play a nominal role at the immediate event when an offender decides to commit a crime. A straightforward yet intuitive depiction of crime, the theory has been particularly effective in explaining widespread and more common offences such as home burglaries and auto theft. The theory diverges from other explanations of crime as it describes when and where a crime is likely to happen but does not answer why offenders commit crime. The theory presumes that the motivated offender reasons their

choices. The key points that constitute the rational offender are highlighted in the following list (Keel, 2005):

> (1) The human being is a rational actor,
> (2) Rationality involves an end/means calculation,
> (3) People choose all behaviour, both conforming and deviant, based on their rational calculations,
> (4) The central element of calculation involves a cost benefit analysis …
> (5) Choice … will be directed towards the maximization of individual pleasure …

Routine activity has been represented in various guises in the field of criminology. It is a basis for crime pattern theory (Brantingham & Brantingham, 2008), which states *how* elements need to come together for a crime to occur. Situational crime prevention, a sub-field within the discipline of criminology, focuses on the prevention of crime, which is principally based on routine activity theory. Situational crime prevention aims to make crime opportunities less attractive for criminals with the objective to prevent crime before it occurs (Clarke, 1995). The situational crime prevention perspective considers resources as an entity that is found along with the opportunity that enables or simplifies the criminal act for the offender. Such a view fails to delineate the difference of offenders that simply stumble upon an opportunity and those that conscientiously conceive new opportunities – understanding causation is tangential. The underpinning focus of crime prevention has been suggested to centre around the straightforward observation that "crime follows opportunity" (Grabosky, Smith & Dempsey, 2001). A less known but relevant model is the conjunction of criminal opportunity (Ekblom, 2001) that offers an extended more elaborate form of the routine activity theory by linking causes of crime with points of intervention. Conjunction of criminal opportunity (CCO) does not compete with other theories but is a framework that draws from pre-existing neo-classical criminological theories with the goal of crime prevention (Ekbom, 2012, p.39). In CCO, a crime happens in the following scenario:

> … a predisposed, motivated and equipped offender encounters, seeks or engineers a suitable crime situation involving human or material targets, enclosures (such as a building), a wider environment and people (or intelligent software) acting as crime preventers or promoters" (Ekblom, 2012, p. 39).

Contrasting to the routine activity theory, CCO explicitly addresses the "equipped" offender (which suggests offender resources), the idea that certain offenders rationally make an effort to *pursue* crime (as opposed to predatory crimes which occur by happenstance when the motivated offender comes across an unprotected victim with no guardians in the vicinity), and notably defines "intelligent software" in the crime scenario (which means software can function on its own as opposed to its use as a simple tool by the offender). CCO offers a pragmatic framework that proposes 11 causes of crime with corresponding intervention strategies - the ordering of these 11 causes has significance with the more immediate (offender-centric) causes being listed first and the later causes (external, situational or environmental) addressing more remote factors. These 11 causes are summarised in the following list along with an example intervention strategy (Ekblom, n.d.):

(1.) Predisposition to offend (possible intervention: early youth involvement)
(2.) Lack of resources to avoid crime (possible intervention: positive role models)
(3.) Readiness to offend (possible intervention: resolve unemployment and give job)
(4.) Resources for committing crime (possible intervention: control access to weapon)
(5.) Decision to commit crime (possible intervention: increase perceived risk)
(6.) Offender presence in situation (possible intervention: divert away from crime)
(7.) Target person or property (possible intervention: value reduction)
(8.) Target enclosure (possible intervention: harden target)
(9.) Wider environment (possible intervention: surveillance)
(10.) Crime preventers (possible intervention: informal and formal social control)
(11.) Crime promoters (possible intervention: tackle criminal subculture)

Offender resources, if interpreted narrowly, are implied in number 4 in the list of 11, however, as summed up in Chapter 7.4, the thesis explores data that can have implications for all 11 points in CCO. Either calculated (CCO) or more opportunistic (routine activity theory), crime is explained as being non-random and it is offender resources that act as a facilitator for crime. Crime may indeed follow opportunity, assuming the rational offender, however, as hypothesised in this thesis, whether that opportunity is realised may also be conditional on resources available to the offender, more broadly it may be predicated on social processes that occur well before the crime occurs and this can begin through participation on web forum sites involved in crimeware activities.

There is a fundamental limitation on the applicability of routine activity theory when describing cybercrime incidents. Yar (2005) underscored the unique spatial and temporal characteristics of the Internet as traits that differentiated cybercrime from crime in the terrestrial "physical" world. Routine activity was originally premised on the idea that convergence occurred in physical space, however, how this convergence translates on the Internet is unclear. For example, an offender does not need to be geographically located in the same country as their victim. Additionally, the notion of time is more complex as an attribute of cybercrime is automation. Attacks over the Internet are essentially pre-set and can occur independently from the immediate control of the offender. For example, an exploit kit is deployed by a cybercriminal on a website that is “programmed” to compromise the computers of unsuspecting visitors.

While the routine activity theory presupposes the rationally thinking offender and may not describe the *causes* of criminal behaviour, its primary usefulness has been its policy implications linked to situational crime prevention. Ontologically parsimonious compared to other criminological theories, the belief was that crime could be simply reduced by removing or altering one of the three elements of convergence, namely the motivated offender, vulnerable target or the lack of a capable guardian. On the view of offenders as opportunistic individuals, other criminologists such as Cornish and Clarke (2014) have pointed out that the rational choice approach (which underpins routine activity theory, crime pattern theory, crime scripts, CCO and situational crime prevention) was revived for the purpose of generating research with practical policy implications.

2.9 Crime Through Association

Crime is learned through social interaction. Sutherland (1947) was among the first to popularise the explanation of how individuals became criminals through a process of social association in his theory called *differential association*. However, it was Tarde (1903) who introduced the idea of crime through imitation, which shared similarities with Sutherland's view, in that criminal behaviour was “acquired” in a social environment. Both Tarde and Sutherland posited that deviant behaviour was imitated through interaction. Tarde viewed

the social environment as the cause of criminal behaviour, according to Wilson (1954). The concept of individuals interacting in a social setting was also central to Sutherland's differential association.

Tarde (1903) believed that the professional criminal went through a "long period of apprenticeship" and "their fate [of becoming a criminal] was often decided by the influence of their comrades" (Wilson, 1954). This notion of a professional criminal was also expressed in Sutherland's (1956) *The Professional Thief* in which he begins to elaborate on his differential association theory that was later published in *Principles of Criminology*. In Cloward and Ohlin's (2013) comments on Sutherland's book, a thief must be accepted by peers, equipped, appreciated, and be able to perform the crime. The implication was that becoming a criminal was not possible for everyone and involved a social process of indoctrination. According to Cloward and Ohlin (2013), one could not become a criminal simply on a whim. It was suggested that certain social environments were more favourable to learning criminal behaviour. In *The Professional Thief*, Sutherland (1956) suggested that professional thieves share "... acquaintances, congeniality, sympathy, understandings, agreements, rules, codes of behaviour, and language" (p. 4) and that normative behaviours existed within social settings of offenders, and to become an offender, an individual would need to be surrounded by such offenders.

Sutherland's differential association theory went through a number of revisions, and in his final release he stated nine postulates in *Principles of Criminology.* To paraphrase the postulates, the theory proposes that crime is learned through social association within criminal group settings where interactions can vary in intensity, the decision to partake in criminal behaviour is based on an individual's definition of "legal codes", and such learning behaviour can also apply to non-criminal behaviour. Regarding the last point, Merton (1938) also grouped criminal and non-criminal behaviour under the same category in his strain theory, which states that it is society that compels individuals to engage in crime.

Other variations of social learning theories exist such as that proposed by Bandura (1977) who applied a similar idea to behaviours using cognitive learning models. Glaser was another theorist primarily concerned with learning instruction in educational environments

(Glaser & Bassok, 1989). Most notably Akers, along with his colleague Burgess, combined the idea of operant condition to Sutherland's differential association theory. Akers expanded on Sutherland's views to include concepts such as differential reinforcement, definitions, and imitation, in addition to differential association (Akers, Krohn, Lanza-Kaduce, & Radosevich, 1979), which is often referred to in criminological literature as "social learning theory" - it should be noted that definitions and imitation are implied in Sutherland's differential association. The addition of differential reinforcement, Akers' term for what is operant conditioning, describes desired behaviour being encouraged or rewarded, while undesired behaviour is reproved or simply unnoticed (Burgess & Akers, 1966). This idea of an individual's behaviour being influenced in a social environment complements Wortley's (2001) concept of precipitators, specifically prompt, pressure and response.

Complementary to Sutherland's theory is the idea that individuals could drift into delinquent behaviour, which was proposed by Matza (1964). Like Sutherland, Matza believed that people learned the values, attitudes, and techniques of criminal behaviour. Additionally, Matza's view of delinquency diverged from strain theory in that he believed that delinquency was more irregular or ephemeral behaviour, rather than a deterministic state where one can exclusively only be a criminal or non-criminal. In Matza's (1964) *Delinquency & Drift*, the underlying message was that current explanations of delinquent and criminal behaviour, at the time, were too deterministic and argues the idea of "soft determinism". The behaviour of an actor is determined by their circumstances that can change. This idea also formed the basis of Sykes and Matza's (1957) earlier neutralisation theory. The neutralisation theory centered on the view that a criminal can decide to *drift* into non-criminal behaviour, and a non-criminal being able to exhibit criminal inclinations. Any individual, not only delinquents, could potentially justify and act out an illegitimate or criminal action. To paraphrase the different approaches of neutralisation listed by Sykes and Matza (1957), the first essentially involves the denial that any illegitimate action has occurred, the second includes abdicating the choice of an action by blaming condemners, and the last involves rationalising an action to be positive or for the "greater good". Matza's view of delinquent and criminal behaviour is consistent with Sutherland's differential association approach, as neither differentiates the processes involved in learning criminal

and non-criminal behaviour. Stressing the significance of temporal order, Wortley (2001) also alludes to techniques of neutralisation, which he refers to as *permit* introduced in Chapter 2.6, and emphasises it as a step occurring prior to opportunity. Such a view of criminal behaviour has profound theoretical ramifications, as any individual could in theory become a criminal.

A major criticism of differential association theory was that it was difficult to operationalise and test (Matsueda, 1988, p. 296). Short (1957) has suggested that differential association theory was untestable as what "definitions" were deemed as favourable, or unfavourable, to law-breaking behaviour was unclear as it could not be quantified in a meaningful way. To test the validity of differential association theory would be difficult when operationalising variables such as "definitions" as used by Sutherland. Cressey (1960) has stated that much criticism of the differential association theory was due to scholars' overly criticising semantics, that is to say, interpreting the postulates of the theory literally. Cressey (1960) also pointed out an ambiguity related to the way in which the social learning process actually takes place, which Sutherland did not clarify.

Interestingly, Sutherland (1947) presented his theory as an alternate explanation of criminal behaviour but did not refute that there may be other approaches to explain delinquent and criminal behaviour. Sutherland classified theories to be either "mechanistic" (individual-centric) or "genetic" (events before the crime) (Akers, 2011, p. 23). Sutherland implied that differential association could explain the processes leading up to a crime.

2.10 Crime and Society

Before delving into the topic of societal views of crime, describing the context functionalism was derived may help to better understand its macro sociological focus. The starting point of functionalist thought began in Durkheim's (1897) *Suicide: A Study in Sociology,*[24] which was the first empirical study that endeavoured to explain social occurrences. Durkheim's study identified that suicide rates differed between countries but within each country remained relatively steady, which led to the inference that suicide was

[24] The original title in French was *Le suicide: étude de sociologie*.

tied to social factors and forces at the societal level.[25] Divergent from Durkheim's past contemporaries, suicide was expressed as a social manifestation rather than a problem inherent within the person that was conventionally viewed as an explanation of suicide. The implications of the study establish the fundamental precepts of functionalism. The key finding was that suicide was evident in all the countries examined in the study, suggesting that there are common social conditions within society that are always present. It was also posited that prior to suicide rates becoming stable that there must be a period of variability or, more fittingly, unpredictability conceivably due to significant changes in society. Normality of a social occurrence and periods in society of instability are the foundational ideas that underlie functionalism.

Functionalism is a perspective in criminology that draws from a number of works from Durkheim, Parsons and Merton. Durkheim viewed crime as a normal part of society. As crime was essentially evident in every modern society, Durkheim argued that crime was natural and played a necessary function in the social order. In a manner, society created what it needed to function, which also includes crime. However, Parsons' view of functionalism stressed understanding the interconnection of the different parts of society and the function of these parts (Adams & Sydie, 2001). Parsons saw a social system as "…a plurality of individual actors interacting with each other" (Parsons, 1951, p. 5) whereby individuals performed roles that ensured such social systems were maintained. Both Durkheim and Parsons were concerned with the function of groups and institutions within society. On the view of crime, Merton's contribution to functionalism was unique. Merton's (1938) interpretation of functionalism was similar to Durkheim's in that both viewed society as composing social entities such as individuals and groups, however, in Merton's view, a state of crime occurred as a result of obstacles and, to overcome such obstacles, deviance was the pathway leading to crime. This state of crime was referred to as anomie. Merton theorised anomie brought about deviance, but Durkheim held that deviance was a result of a breakdown of norms, two clearly distinctive views (Hilbert, 1989, p. 242).

[25] Durkheim (1897) posited three explanations of the cause of suicide. An in depth analysis of these postulates will not be provided, however these are briefly described as follows: "egoistic suicide" results from lack of attachment and acceptance in society, "altruistic suicide" is best illustrated as influence from a higher authority, for example fundamentalist terrorist groups and religion, and "anomic suicide" generally results from an absence of rules in society that in turn causes confusion and disorder.

There have been a number of criticisms of the functionalist view of crime. Functionalism appears to be logically flawed because it is a teleological argument (Isajiw, 2013). For example, a functionalist would argue online fraud to be perpetrated by criminals for personal enrichment, and the only way for criminals to obtain large sums of money would be to engage in online fraud. A cause and effect explanation would view the same situation differently, in which criminals with no legitimate avenues for income requiring money needs to commit crime to obtain money, and the only way for them to obtain money is to engage in online fraud. Another often-raised criticism has been that functionalism overlooks the role of individual action. In other words, individuals are only seen as being important when they are a part of a social system (Ho, 1998). In the crime scenario, functionalism would not be able to give an explanation of the actions by the individual agent, for example, a solo hacker that breaks into a computer system over the Internet for some nefarious reason, as the emphasis is on describing larger scale social processes. Functionalism faces limitations in explaining social situations and is unable to address individual motivations for crime. Another limitation is that functionalism is unable to address the changes in the function, or the creation of new ones, that a particular group serves in the larger social order. For example, modern law enforcement is known to have originated from early forms of kin policing[26] where citizens were ultimately responsible for maintaining order among their own relatives or social group. Law enforcement, as the institution as it is known today, did not exist in the past. Functionalism may explain a function at the time it is present (e.g., kin policing when it existed in the past), but does not address how such functions evolve (e.g., the growing paucity of kin policing and the formation of the social institution of law enforcement that is empowered by the state). [27] Functionalism principally emphasises stability and equilibriums of social systems and society as a whole.

[26] *Kin policing* is sometimes referred to as tribal or family policing. It is used as a means of social control in which social groups are held responsible for actions of its members (Reith, 1975).
[27] The limitation highlighted centres on the function itself that changes for a social group. This should not be confused with rapid changes in society, which was raised by Merton (1938) who expanded upon functionalist thought when explaining that it was the *rapid* transformations in society that caused anomie, which he referred to as "dysfunction". It should be noted that Parsons' (1951) version of functionalism did address such changes in his AGIL model (adaptation, goal attainment, integration latency), which explains how social systems survive.

Extending on Merton's anomie, Messner and Rosenfeld (1994) argued that certain institutional structures dominated over others (for example, family or political groups) that were less capable of insulating its members from anomie. The imbalance of structures is compatible with conflict based criminological explanations that arose largely from literature from the revolutionary sociologist Karl Marx.[28] Conflict-based explanations of crime share the common idea that society exists, not as an equilibrium or by consensus stipulated by the functionalist approach, but due to consistent conflict between certain values or groups within society. The functionalist may argue conflict to be normative and a required aspect for society to function. In conflict based explanations, societies are recognised as dominated by a powerful elite while some groups are coerced and oppressed, with individuals from afflicted groups engaging in crime due to the unequal distribution of power. The German sociologist Max Weber,[29] who also shared similar ideas of Marx on conflicts in society, diverged in how he defined the sources of conflict (Morrison, 2006). Marx's view of conflict occurred between two classes, the rich versus the poor. In Weber's view, conflict could arise between any social groups within society. Additionally, the law is seen as an instrument for the powerful to control the less powerful in conflict based explanations of crime. Weber also viewed criminalisation as an instrument to safeguard the interests of the powerful, in which he states, "criminality exists in all societies and is the result of the political struggle among different groups attempting to promote or enhance their life chances" (in Bartollas, 2005, p.179 as cited in Walsh and Ellis, 2006). In the interpretation by Vold, Bernard and Snipes (1998), it was the competing interests of groups that created conflict. Among the different views, it is the uneven distribution of power that underlies the cause of conflict. A major criticism of conflict-centric explanations of crime was that it overly emphasised the "financial" interests of the powerful (Carl Klockars, 1980 as cited in Hagan, 2012), as power is often associated with money.

[28] *Karl Marx*, philosopher and socialist, is best known for his published work such as *The Communist Manifesto* and *Das Kapital*, which have been used to develop Marxist philosophy. Marxist based theory argues that the imbalance of material wealth, forming a rich and poor class, in society creates conflict.

[29] Weber, along with Durkheim and Marx, are often stated to be the founders of sociology.

Branching off from macro social based explanations of crime are subcultural theories. Subcultural explanations of crime describe the formation of delinquent groups. Drawing from Merton's (1938) strain theory, which explained crime occurring as a result of the inability to attain monetary success in society, it was Cohen (1971) who developed subcultural views of crime to explain the non-rational[30] nature of delinquent gangs. Yar (2005a) pointed out that hacking communities could be viewed as a subculture, suggesting that activities associated with such communities should not be viewed as criminal but as a collection of individuals with shared values and behaviours that are simply different from those of mainstream society. To explain criminal subcultures, Cloward and Ohlin (1994) extended on Merton's view, which was described as *differential opportunity*, and proposed that there was an illegitimate opportunity structure for every legitimate opportunity; the implication of such a view would mean that crime is dictated by the accessibility of illegitimate opportunities and structures to the potential offender. Cloward (1959) believed that knowing these illegitimate opportunities required a process of social association in "criminal learning environments … [with a new offender eventually] inducted into criminal roles " (p. 169), which was used as a basis to explain the formation of criminal subcultures.

There are also social mechanisms that work to dissuade offending behaviour that should not be overlooked. In Hirschi's (1969) social control theory, it is attachments to social norms, family and peers that are argued to discourage the individual to commit crime. A similar line of point was raised by Felson (1986) who proposed the role of the "intimate handler", an individual with influential control that dissuades the offender from crime (p. 60). Forces that work against offending behaviour are similarly noted in Ekblom and Tilley's (2000) discussion on offender resources in which it is stated that there are "resources for avoiding committing crime" (p. 381), and is also addressed as "lack of resources to avoid crime" in Ekblom's (2005) CCO.

2.11 Using Routine Activity Theory to Explore Offender Resources

[30] Non-rational activities include crime that may not necessarily be driven for the underlying motivation of profit such as vandalism and theft of cars for joy riding.

As introduced in Chapter 1, Ekblom and Tilley (2000) highlighted the importance of the theoretical concept of the resourceful offender, although it was in Cohen and Felson's (1979) initial proposal of the routine activity theory that implicitly covered this general idea when describing offender ability. In Ekblom and Tilley's (2000) explanation, an offender would need to be properly resourced, or supplied with the necessary means, in order to realise a crime. Essentially a concept that places an emphasis on the likelihood of a motivated offender engaging in crime, an offender needs the ability, know-how, or tools to carry out a crime, and in some situations collaboration with co-offenders is necessary, some of which is compulsory for an offense to be ultimately committed. Premised on the view of offenders as individuals seeking gain, perpetrators are viewed as deliberate thinkers when weighing out the rewards and risks of crime whether that includes merely stumbling upon an opportunity, actively searching for potential opportunities, or creating new opportunity that did not exist previously. Access to resources, at hand to an offender, was posited to play a factor whether a crime was to occur and for its success. The investigation in subsequent chapters will focus on examining offender pathways leading up to the event of a cybercrime with the attention placed on crimeware. When examining aspects of learning, Sutherland's differential association is the primary focus, however elements from relevant learning theories may be explored, more specifically Sykes and Matza (1957) techniques of neutralisation, Burgess and Akers (1968) differential reinforcement theory and Akers' (1973) version often referred to as "social learning theory" which is essentially a composite borrowing elements from Sutherland's differential association, Akers' own differential reinforcement and an emphasis on definitions and imitation.[31] The thesis draws from all these theories from the 'social learning tradition'. Rational choice, routine activity theory, crime scripts, Wortley's two-stage model and precipitators, CCO, and situational crime prevention can be considered as general opportunity theories in the study, although certain theories have additional emphasis in other aspects, such as *causal factors* (crime scripts, Wortley's two-stage model and precipitators, CCO) and *intervention* (situational crime prevention, CCO). An ostensibly different paradigm, an examination of the role of

[31] Some modern scholars may supplant Sutherland's differential association theory with Akers' social learning theory. Watts, Bessant and Hil (2008, p. 60) have commented that Sutherland's differential association theory is an elaboration of Tarde's notion of imitation. Akers' version could also be viewed as an extension of Sutherland's differential association theory, with the added concept of differential reinforcement in addition to their attempts to operationalise the theory for empirical testing.

crimeware relative to the wider cybercrime landscape and society is presented that draws from functionalist thought, law and social systems.

In this thesis, a range of criminological theories is drawn upon to advance the concept of offender resources introduced by Ekbom and Tilley. Crime is complex and its causes are unlikely to be explainable by a single theoretical approach. When studying crime, "we must take into account several dimensions of social reality" (Barak, 1998, p. 6). A multipronged view of cybercrime may impart not only a more comprehensive explanation but also provide new insight. To re-emphasise a key objective of this thesis, the research endeavours to draw from relevant theories in criminology in order to propose a conceptual model of offender resources.

The next chapter provides details on the methodology and data sources used in the research.

Chapter 3: Methodology

> The world is full of obvious things which nobody by any chance ever observes.
>
> *~Arthur Conan Doyle*[32]

This chapter provides a recap of the research objectives and explains the methodology used in the thesis. The research centres on data collected using a common approach in sociology research known as non-participant observation. As a supplementary source of data, it also relies on a qualitative analysis of interviews with frontline investigators, electronic data gathered by third party agencies and relevant examples from secondary sources. Details on the methods of selection of data, the research design and the method used to interpret the data sources are covered in this chapter.

3.1 Foundations and Assumptions

The nature of the knowledge produced in this thesis is largely based on qualitative methods with a core component using observation as a means to collect data. It is also recognised that what has been chosen to be observed is somewhat more a subjective choice or conditional on what may be observable. The notion of falsification through replication is paramount in this research. For example, if we claim all cybercrime perpetrators use hacking tools, confirmatory evidence cannot prove that assertion to be true. However, contradictory evidence can prove the claim is invalid. Moreover, an objectivist point of view is taken in relation to the analysis of the data in this thesis. Inquiries from different independent observers examining similar data, using alike techniques of analysis, should result in comparable empirical findings. On the other hand, explaining the data using criminological theories, that can be interpreted differently, might produce different explanations of online criminal behaviour. Objectivity, an often-raised limitation of qualitative-based studies, can always be questioned as the choice to focus on using one approach, or a specific theory or theories, over another is in inescapably influenced by the

[32] Quoted from *The Hound of the Baskervilles* by Arthur Conan Doyle (1998, first published in 1902).

researcher's background (Kuhn, 1977). As the sole researcher, I recognise that there are always limitations, which should be addressed to the best possible extent although it may not be feasible to address every limitation.

Cybercrime is recognised by many scholars to be a social construct of society. It is through social mechanisms, such as the legislative process and interests of different groups and those in power, that criminal laws are created to delineate what is socially acceptable and proscribed (Quinney, 1970, p. 11), and the Internet is no different. Scholars of crime, in particular those trained in the field of sociology, often view crime as a form of deviance described as "... any non-conformist behaviour which is disapproved of by society or a social group, whether it is illegal or not" (Browne, 2011, p. 234). Formal illegality does not sufficiently define such behaviours, as deviant behaviour can be lawful (e.g., tolerated yet not proscribed). The downloading of copyrighted movies, as an example of deviant behaviour, is currently illegal in the case of Australia, although this was likely not the case in the past when legal precedent was lacking and no laws existed criminalising such activity. To provide another example, the drug smuggling ring of unregulated AIDS medication in the mid 1980s *Dallas Buyers Club* venture was not explicitly illegal but was contested by the US Food and Drug Administration (FDA); AZT was a drug treatment that was originally trafficked and later approved by the FDA (Minutaglio, 1992). Furthermore, the interpretation of "crime" is subjective and arbitrary that is subject to definitional contests (Barak, 1998, p. 21). This is perhaps even more the case on the subject of the Internet and cybercrime, which in many respects is a still a novel development both in terms of technology and social adaption to this technology.

In this thesis, cybercrime is framed as deviant behaviour on the Internet and may also be expressed as cyber deviance, that is, atypical behaviour in relation to that of socially accepted normal behaviour characteristic of the *mainstream*. Certain behaviours and actions will be considered criminal if it adversely affects a third party, for example, when malicious actions by an individual are directed towards computers connected to the Internet and its users. This definitional distinction of crime and deviance concerns the creation and distribution of crimeware tools. The legitimacy of whether crimeware should be defined as

lawful has been contentious in countries like the UK[33] and Germany,[34] which have potentially banned all malware tools and programs. The existence of crimeware tools conceivably derive for reasons rooted in curiosity, legitimate and justifiable aims, or mischievous intentions, if not overtly for crime. It is apparent that its wider propagation and use, in cases when it is involved in the commission of cybercrime, is clearly unfavourable to the victims as in the theft of personal private information used for fraud. Crimeware is typically assumed to be the result of actions of cybercriminals, which in many instances may be true, but certain actions connected to crimeware may not be intentionally malicious or intended for a criminal purpose. For example, the case where a legitimate security researcher, who possesses such software, examines how it works to figure out how to better protect Internet users. Not all crimeware, and its associated activities should assumed to be "criminal" as the motivations of actors may not be for the purposes of wrongdoing in all cases.

It is also unclear whether individuals who participate in criminal activity in the online environment differ from "conventional" criminals outside of the Internet. Few scholars have challenged such views of whether cybercrime is the same, or simply a modern extension, as crime of the past before the Internet existed. Jaishankar (2008) theorised that people behave differently in virtual environments than they do offline suggesting that individuals may have multiple personas. For example, an individual may be a law-abiding citizen offline but have criminal inclinations when operating within the domain of the Internet. Inquiry into exploring how online deviance, an aspect of which is examined in this research, relates to offline circumstances is beyond the scope of this research. Although the research is based on observation, such observation is confined to what is visible on the Internet and reasonable inferences can only be made to describe online behaviour.

---

[33] Under the *Computer Misuse Act* 1990 (UK), amended in the *Police and Justice Act* 2006, an individual that "makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, [the unauthorised access of a computer]" is illegal. Additionally, "article" is defined as "any program or data held in electronic form".

[34] In German penal law, Section 202(c) criminalises offences that involve "producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible … software for the purpose of the commission of such an offence" as translated from German by Prof. Dr. Michael Bohlander at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1754

3.2 Revisiting the Research Questions

The aim of this study is to expand upon the offender resource concept by reviewing the applicability of a selection of theories from the discipline of criminology. As outlined in Chapter 1, offender resources encompass a range of elements depending on the nature and goals of the cybercriminal. The thesis will only focus on online interactions and behaviours that are specifically crimeware related.

The availability of resources for offenders is believed to be one of the sources, and causes, for widespread offending activity. The use of offender resources, such as software designed for crime and various illegitimate online services, are claimed in many computer security industry reports to play a contributory part in increasing incidents of cybercrime. Accessible to all types of actors from curious delinquents to proficient criminals, such software facilitates online crime and other activities of a malicious nature. The research questions are re-stated as follows:

Research questions

(1) What are the online social dynamics and behaviours among offenders?
(2) To what extent can offender interactions be explained as rationally driven processes?
(3) Where do online offender communities fit in the wider social order?
(4) How do the selected theories in the study interconnect to explain the online behaviours examined?
(5) What is a feasible theoretical model that describes offender resources?

The focus of the first question is on individual social agency. Chapter 4 investigates the social processes and the role of learning within select web forum site communities.

The second question explores the motivation and intention of offenders. Chapter 5 examines the rational nature of the offender decision-making process based on what can be inferred from the discussion content and the features of crimeware being circulated.

The third question involves an analysis of offender communities as a social system from a macro perspective. Chapter 6 examines criminalisation, how law is perceived among web forum site members, as well as the relationship between offenders and other groups and institutions in society.

The fourth and fifth questions are discussed Chapter 7. The analysis of the web forum sites involve assessing ways in which traditional criminological theories can be used as an explanation of online criminal behaviour. The goal is to present a conceptual model of offender resources.

The research relies on the analysis of content from web forum sites and is the primary source of data. Interviews with key individuals from Internet response agencies, electronic data generated from crimeware are also investigated, and recent examples reported by the media are included.

3.3 Starting the Research and Background

Before elaborating on the methodological aspects of the thesis in detail, I present what occurred in the earlier phase of the research. The background work completed towards this thesis, although not directly useful as a source of data, is important to understand the choice of methodology used. The preliminary stage of the research involved informal discussions with key Internet crime response and mitigation agencies from government, the non-profit and the private sector. In the first 18 months of the research, I had met with and spoke to 84 individuals from 20 institutions involved in responding to cybercrime in some capacity - some of these individuals were subsequently interviewed and used as a source of data in this thesis. My decision to focus on crimeware was influenced due to these meetings and has guided the research. General issues identified, from the meetings, related to incidents occurring over the Internet and included the growing prevalence of botnets, banking and credit card fraud, hacking incidents of websites and the theft of private data. These early discussions have been crucial in keeping up-to-date on current forms of cybercrime and the challenges to respond to online crime.

The research process was supported with the help of research colleagues at the ANU Cybercrime Observatory. As a PhD student, I was fortunate to have the opportunity to be a part of a research team that had previously established relationships with crime prevention agencies locally and overseas. A number of these agencies offered data that was used in this research. The relationships with the organisations were opportune to gain access to data feeds, as well as recent samples of crimeware tools.

The decision to proceed with the topic of this thesis was veritably influenced by my educational background and past experiences. As a researcher originally coming from the discipline of computer science, I was drawn to exploring the crimeware process from the point of view of software development. Examining the technical underpinnings of the software stemmed from curiosity rather than an academic pursuit of interest at the beginning. I was interested in understanding the functioning of software, its architecture and features, which in a certain respect appeared clever and elegantly designed, and was particularly intrigued with how the software was able to evade detection from victims and security protection products. In the first year of the research, I had spent a considerable amount of time experimenting with crimeware tools that I was able to collect through sources; this involved running botnet simulations in a secure computer lab to decrypting encrypted malicious files containing botnet instructions from cybercriminals. My initial goal was to understand in greater depth how crimeware tools operated from a technical standpoint. This work was carried out in collaboration with research colleagues that specialised in computer security as well as criminologists.

Although not covered in this thesis, the effort to analyse the technical workings of the software has proven to be useful to identify and distinguish the crimeware tools disseminated on the Internet.[35] Over time I had identified those crimeware tools that were in higher demand, how to use them, and where to go online for technical support. The research also lead to the embarking of applying new techniques in crime research, some of which were useful to parse[36] the electronic data from data providers, and less applicable in

[35] This work was undertaken at the ANU Cybercrime Observatory at http://sociology.cass.anu.edu.au/centres/anu-cybercrime
[36] To extract, break down and describe the data.

explaining criminal behaviour and interactions. In an effort to analyse the large quantity of data, novel large-scale data analysis techniques and custom tools had to be developed out of necessity. The electronic data provides certain insight into the intentions of cybercriminals. This data is referenced in this thesis as a source for illustrative purposes (see Case 4 and 5 in Chapter 5) but has not been systematically analysed as it is beyond the scope of the research goals.

Other approaches were considered to collect data. These consisted of surveying active offenders on the Internet, setting up a honeypot with the aim to capture live malicious Internet traffic, and actively engaging in the purchase and procurement of services, provided by offenders, relevant to crimeware and botnets on web forum sites. Mainly due to time limitations to complete the PhD research, a non-participation observation approach was used as the primary source of empirical data. The other approaches may be explored further in future research initiatives after the PhD.

3.4 Non-participant Observation of Web Forum Sites

This section describes where and how the main source of empirical data of this thesis was collected. The research uses a non-participant observation methodology to collect data. Non-participant observation is a common technique used in social science research to observe social interactions first hand in which, "the researcher enters a social system to observe events, activities, and interactions with the aim of gaining a direct understanding of a phenomenon in its natural context" (Mills, Durepos & Wiebe, 2009). In Gold's (1958) classification on roles of the observer, the "complete observer" approach is listed, as a type of observational approach in which there is no engagement with the target population being observed. The study centres on data collected through observation from a key selection of web forum sites associated with activities relevant to crimeware, botnets and hacking. A grounded theory methodology was subsequently applied to identify common themes from the data collected (Glaser & Strauss, 1967). The web forum sites in the study were publicly accessible with only English language based sites examined. The actual dates of discussion content from the web forum sites span a period of four years from 2008 until the time of

data collection in March 2012. Refer to Appendix 3 for additional insight into the data collection and coding process.

Web forum sites as a source of data has been used in research when observing underground communities involved in fraudulent activities (Holt, Strumsky, Smirnova, & Kilger, 2012; Holt, 2010; Décary-Hétu & Dupont, 2012; Soudijn & Zegers, 2012). Web forum sites, also commonly referred to as "Internet forums" and "discussion forums", are a form of computer-mediated communication (CMC), which also include instant messaging, chat rooms and email (Thurlow, Lengel, & Tomic, 2004). As a CMC, web forum sites have distinctive characteristics that separate it from other communication systems that include the following:

- an extended duration of time can pass between communications, as web forum sites are asynchronous similar to emails,
- identities are anonymous whereby participants are identified by aliases that they create, and
- messages are persistent, that is, a message that is posted is essentially permanent unless explicitly deleted (a unique attribute that makes web forums different from chat rooms).

The eight web forum sites selected are a convenience sample. Four of the eight web forum sites were selected each using a different search engine: Google, Bing, Yahoo and Ask. Holt and Lampke (2010) used a similar technique when identifying web forum sites involved in the exchange of stolen data. To obtain locations of web forum sites, the terms "hacking tools discussion forum" and "malware forums" were entered in each search engine. The top site retrieved from each search query was included to the selection of sites. An additional five web forum sites were subsequently selected using online polls[37] posted on each of the previously selected four sites with the question: "Which forum do you visit the most for hacking, malware and botnet tools?" There were a total of 24 responses among the four online polls, which was left up for two weeks. The top five web forum sites from the online polls were added to the initial sample set. It should be noted that two of the sites

[37] An *online poll* is an opinion poll where participants are self-selected. Online polls are nonprobability samples.

were later removed from the study, as they were no longer accessible in the midst of the data collection process. One site was reported as being taken down by law enforcement and the other site was shut down for unknown reasons. An additional web forum site was arbitrarily selected that was hosted on the Tor[38] network. The selection approach clearly does not provide for a probabilistic sample. However, an effort was made to obtain a relevant mixture, if not a comprehensive capture, of web forum sites active at the time of investigation (see Table 1 below).

Table 1: Breakdown of web forum sites

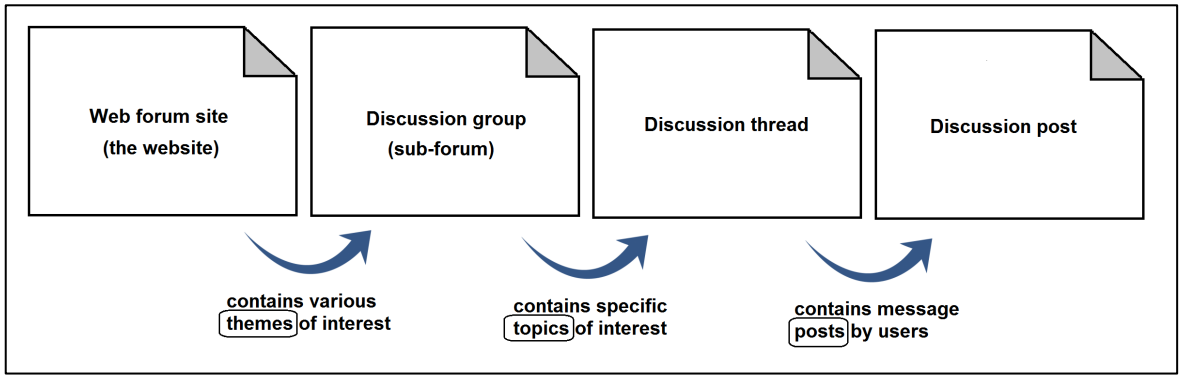
Web forum site	**Total number of registered users**	**Total number of discussion groups selected**	**Total number of discussion threads selected**
A	100,000+	7	350
B	50,000 - 100,000	1	50
C	50,000 - 100,000	6	300
D	10,000 - 50,000	2	100
E	10,000 - 50,000	5	250
F	10,000 - 50,000	1	50
G	10,000 - 50,000	1	50
H	+100,000+	6	300
		Total: 29	Total: 1450

Each web forum site consisted of multiple discussion groups (see Figure 4 below). On credit card fraud web forum sites, Yip (2011) recognised that each "sub-forum", or discussion group, was distinct each with a different focus. A web forum site may lure a specific audience, however, each discussion group conceivably attracts different visitors as the focus of discussion groups can vary. From eight of the web forum sites, discussion groups were purposefully selected that were only relevant to crimeware tools. Some sites contained discussion groups irrelevant to the scope of the study, such as gaming and general topics on software development practices, and were thus omitted. The selection

[38] *Tor*, or "The Onion Router", is a communication network on the Internet that allows users to hide their location, traffic and the location of hosted websites. Tor was designed to protect the privacy of Internet users. Tor is commonly associated with criminal activities such as the trade of illicit drugs and child exploitation.

process of discussion groups was determined based on the title of the discussion group and its description. Examples of discussion groups include those that were relevant, or contained some related discussion, to crimeware such as “tools”, “botnets”, “hacking”, “tutorials” (related to tools, botnets or hacking), or solicitation of relevant services. Additionally, discussion groups captured included those that covered encryption[39] and exploits[40] as they contained discussion content relevant to crimeware.

Figure 4: Web forum site structure



A “50-15-10” sampling strategy was utilised. Among the selected discussion groups, the top 50 discussion threads were selected. If a discussion group contained further “sub” discussion groups beneath it, 15 additional discussion threads were selected from these. Lastly, the ten most recent discussion posts were selected from each of the selected discussion threads. The sample size selection process was not arbitrary and involved an iterative process. For example, the initial pass of data collection on the first few web forum sites involved capturing all discussion threads under a discussion group. This lead to capturing too much data feasible for analysis, and for this reason the number of discussions threads had to be reduced. Capturing all the discussion posts for each discussion thread also led to capturing too much data. The collection of discussions posts had to be limited to a manageable size, and had to be reduced further. Furthermore, different sampling strategies were attempted such as searching for specific keywords to identify discussion threads and

[39] *Encryption* is used as a technique to hide malware from being detected by its targeted victims and anti-malware security products.
[40] *Exploit code* is a sequence of code that aims to take advantage of a vulnerability of a system. The goal of a cybercriminal would be to gain access into a system using such code.

web scraping[41] all discussion content. The aim was to collect only relevant discussions with a wide cross-section of discussion threads. It was determined that a total of about 1,500 discussion threads, which consists of approximately 15,000 discussion posts, was the maximum manageable size feasible for analysis, that is, by a single researcher. The "50-15-10" sampling strategy was optimal to achieve this goal. Using this strategy, the main page of the web forum site, discussion groups, discussion threads and discussions posts were downloaded and saved one by one onto a computer for offline analysis.

Importantly, it is the discussion posts that contain the key data, which reveals the interactions and exchanges between different individuals communicating online. A discussion thread can comprise many discussion posts, and in some cases there may be little to no discussion activity in a discussion thread. Discussion threads have a distinct structure and can be represented as conversations with the following features (Resnick, Hansen, Riedl, Terveen, & Ackerman, 2005 as cited in Ackland, 2013):

- a set of topics or groups where the threaded conversation occurs,
- within each topic there are threads: top-level posts and responses to those posts,
- each post in a thread is authored by a single person,
- posts are typically permanent, and
- users are generally presented with the discussion thread in reverse chronological order.

Examples of discussion content are presented in subsequent chapters based on identified themes. For example, if a theme related to profit gain as a primary motivation of activity, an example of discussion content is shown that is relevant to this theme. Further examples under the same theme are provided if they reveal additional observations or findings of importance to explain certain behaviours. It should also be noted that certain examples might be applicable to multiple themes. For example, a discussion thread may suggest profit as a motivating factor of certain behaviour as well as reveal elements of trust playing a role in interactions. In these cases, the discussion thread or post is interpreted and

[41] *Web scraping* is an automated technique which downloads all content from a website by visiting and downloading every webpage.

explained only in the context of the theme being examined in the particular part of the chapter.

Other approaches were considered in conjunction with thematic coding, such as generating frequency distributions of the most used terms. Examining keywords was useful in revealing common words used but did not take into account meaning, which could only be analysed by manually reviewing the discussion content.

In this thesis, the discussion content is presented in a condensed form and modified from the original format as it was shown on the web forum site. The following is an example of the format used to display discussion content in subsequent chapters (skip to Figure 5 to view how a discussion thread is structured with time taken into account):

> [Title]: This is the title of the discussion thread
> [OP]: This is the first post made by the original poster, or the OP … [Download link of a tool] …
> [R1]: This is the first response.
> [R2]: This is the second response.
> [R3]: This is the third response.
> [R4-OP]: This is the fourth response, which is also made by the OP.

Figure 5: Structure within a single discussion thread

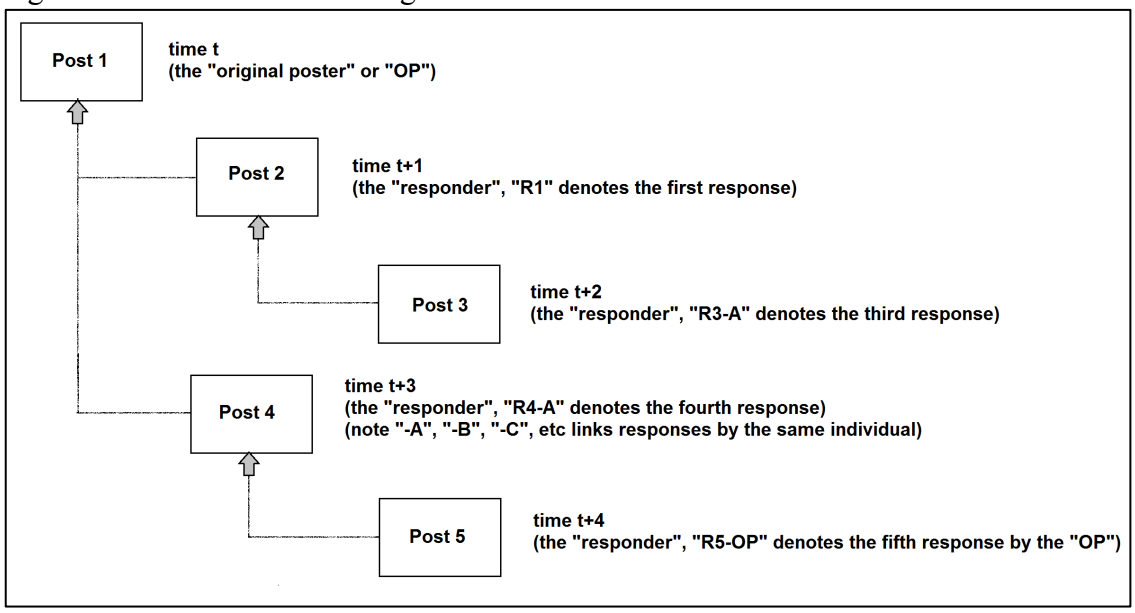


Figure 5. Diagram of a discussion thread. Modified version from "Web social science: Concepts, data and tools for social scientists in the digital age", by Robert Ackland, 2013.

Showing entire discussion threads in most instances was not feasible due to excessive length. Certain parts of a discussion threads were truncated for this reason, which is also the reason why only the top ten most recent discussion posts within a discussion thread were captured. When showing a discussion thread in the thesis, a post is omitted if the response is irrelevant to the discussion or unrelated to the theme being identified. This was done to highlight only pertinent discussion content. To signify discussion posts in which the OP replies to their own discussion thread, "-OP" is appended to the response label, for example "[R4-OP]" denotes a response by the original poster (OP), which also denotes that it is the 4th response (or the 5th post if you include the first post by the OP). Multiple responses by the same individual are similarly denoted with a letter, for example, "[R3-A]" and "[R4-A]" would be a post from the same member. The thread title, represented as "[Title]", is omitted if duplicated within the first post by the OP or if the thread title is non-specific. An example of a non-specific title would be "Tool for download" or "I have a question". Summarised descriptions are provided such as "[Download link of tool]" or "[List of tools]" within square brackets when appropriate. Also, "…" is used to signify there was additional content that was removed, which was done to reduce the length of the text. Some posts were on multiple lines - these were combined into a single line in certain cases to save space on the page and for presentation. A relatively large proportion of discussion content required concentrated efforts to read due to grammatical errors and spelling mistakes. For this reason, a certain level of grammar and spelling had to be updated for ease of reading and comprehension. Revealing original text as shown in the web forum site post, in most cases, would have made the presented discussion content difficult to read. The text was edited carefully to avoid inadvertently changing the semantics of the discussions. The discussion content is consistently presented in this thesis and may be grammatically modified from its original version.

The thematic coding used is based on a recent field of research that concerns online learning. Before explaining the coding process, I highlight some of the limitations of the social learning tradition of criminology. One criticism of Sutherland's differential association theory was that operationalising and testing it was difficult (Matsueda, 1988, p. 296). If one considers the fundamental idea of learning as a social process, the question

arises how such a process could be recognised and, more importantly, how interactions involving learning related interactions could be examined. Learning is considered subjective and, consequently, can be difficult to study without observing social interactions first hand. Even if one were able to view such social interactions reminiscent of learning, it is not clearly evident what social markers or behaviours to look for. It was Akers (1977) himself, a major proponent of learning theories of crime, who suggested it was unclear what "learning" actually involved. Tarde, one of the early crime scholars to bring up the idea that criminal behaviour was learned, suggested that learning occurred through imitation, however learning behaviour by simply replicating another individual's behaviour is a narrow conception of ascertaining social learning.

Holland (1984) stated one of the reasons empirical scholars have questioned differential association theory was due to the lack of clarification of the idea of "definitions [of the legal codes]". Definitions favourable to *act out* deviant and criminal behaviour can vary depending on the individual or group, as well as other factors such as time and place. In the observation part of the study, we take it as a given that such definitions exist, that is, there are factors, beliefs and conditions that may lead an offender to behave in a certain manner that may be deviant, which may also be illegal, although these definitions are likely to vary among web forum site participants. The investigation in Chapter 6 will reveal that definitions based on legal codes, or the awareness of what is legal or illegal by an individual, is not as definite as other types of crimes.

The question now arises whether deviant behaviour can be observed online. Aspects of social interaction and learning are evident, and to various degrees are observable, on CMCs such as web forum sites. Although there is no physical or face-to-face contact, there are certain characteristics of web forum sites that allow online forms of interaction to be observed due to certain traits, which may not be possible when examining the learning process taking place in *terrestrial* interactions. Web forum sites are asynchronous, where multiple users can engage in discussion with others in which one member can respond to another member after a period of time has elapsed. Additionally, interactions are persistent as the posted messages are, for the most part, permanent and do not disappear. In a sense,

these features allow online interactions to be recorded, essentially giving us a *snapshot*, which allow interactions to be viewed at a later point in time.

During the process of examining the web forum sites, various aspects of learning were visible. However, there were challenges as there was a lack of models and research techniques within criminological research discourse to assess whether learning theories could be operationalised for interactions taking place in the online environment. For this reason, the research field of online learning systems was used as a guide in the thematic coding process.

De Wever, Schellens, Valcke, and Van Keer (2006) suggested that theories related to learning could be operationalised and applied to asynchronous web forum sites, the same sort of sites examined in this research. Schrire (2006) described various dimensions of learning, which were: interactions among members, the character or the content of discussion, and the cognitive process of individuals and groups. The first two of these, namely, interactions between members and the content of discussions are examined in this chapter. Based on research of online interaction among students, Soller (2001) proposed a taxonomy called the Collaborative Social Learning Skills Taxonomy (CSLST). The model focused on examining real-time problem solving processes, which was adapted from McManus and Aiken's (1995) Collaborative Skills Network. The CSLST provides a list of possible indicators that involve aspects of *collaborative learning*. Learning processes were broken down into three main categories, that is, *creative conflict*, *active learning*, and *conversation*, which are further broken down into sub-categories. A simplified version of the CSLST was adopted to assist in identifying relevant themes connected to learning (see Table 2). New codes were subsequently created to identify additional themes found in the web forum sites. The CSLST was used primarily as an initial guide to establish whether learning was taking place.

Table 2: Modified version of the Collaborative Social Learning Skills Taxonomy codes

Code groups	**Codes**
Creative conflict	Teacher mediation, agree, alternative, conciliate, disagree, doubt, exception, infer, suppose
Active learning	Encourage, reinforce, assert, elaborate-inform, explain, justify, lead, resources, suggest, assert, clarification, elaboration, illustration, information-request, justification, opinion-request
Conversation	Accept/confirm, appreciation, reject, apologize, attention, listening, request confirmation, suggest action, coordinate group process, focus change, present, summarize information, end participation
New themes	(Not listed in any order) Reputation, lack of trust, deception, target other members, target external sites, development, innovation, open source, private source, collaboration, exchange (monetary), exchange (software), exchange (services), exchange (1:1), helpfulness, effectiveness, ignore, barter, solicitation of services, searching of services, rent, "try and buy", tinkering, assistance, tutorial, practice, testing, research, curious, value, law (questioning), morality (questioning), boredom, ideology, amusement, skill honing, tool (remote access trojan), tool (crypter), tool (keylogger), tool (exploit kit), tool (exploit), botnet, vulnerability

Note. Simplified version of the CSLST, from Soller (2001), which contain three code groups: creative conflict, active learning and conversation. The "*New themes*" code group is not from the CSLST, and was added using the grounded theory method. After thematic coding, the themes were grouped.

Lastly, a three-page glossary of key acronyms and jargon containing brief descriptions has been included (see Appendix 2). Explanations of certain terms found in discussion content are included as footnotes throughout the thesis and may also be duplicated in the glossary.

In this thesis, the assumption is made that online social learning processes of deviants and criminals are similar to those involving non-criminal learning behaviour. Sutherland (1947) suggested that learning criminal behaviour involved the same mechanisms as other forms of learning. In other words, the processes of learning criminal and non-criminal behaviour were alike.

3.5 Interviews with First Responders

As an additional source of data, interviews were conducted with Internet first responders involved in monitoring or mitigating cybercrime activity. The interviews were open-ended which presented a single starting question: "Can you tell me anything about cybercriminals involved with using malware tools or botnet tools in your field of work?" From this

question, there were additional follow-up, probing and specifying questions ("Strategies for Qualitative Interviews", 2014) to persuade the interviewee to provide further details: "Could you please elaborate? Can you provide examples? Can you please clarify? What do you mean by that? Is there anything else? What happened?" These probing questions were continually asked after each response until an hour elapsed or when the interviewee desired to end the interview. Furthermore, if a line of discussion led to little information or revealed few details, a question was asked to elaborate on a previous point that was raised: "Very interesting. A minute ago you mentioned _____, can you tell me more about that?" A total of 12 individuals were interviewed using this method which are grouped under three categories, namely public sector, private sector and independent (see Table 3). It should be noted that two of the interviewees revealed in the interviews that they were former blackhats[42] and were involved in illegal activities before moving onto legitimate roles. The interview results are predominantly found in Chapter 6.

Table 3: Breakdown of interviews

Category	**Number of interviewees**
Public sector	3
Private sector	4
Independent professional	5

The interview approach was purposefully designed to be as unstructured as possible with the goal to encourage the interviewee to freely bring up issues of importance, with minimal influence from the interviewer. The probing questions provided enough direction as necessary to draw out information (May, 1991, p. 191). Additional interviews could have been done, however, the aim was to focus interviews with crimeware specialists involved in hands-on investigations. The interviewees were required to meet explicit requirements to be counted in the study, which include having at least five years of direct experience mitigating activity specific to crimeware (software tools) and can also encompass investigating activity *generated from* crimeware such as botnets and stolen data linked to certain types of crimeware, their duties must involve hands-on investigations at least 16 hours (two days) per week, and they must be currently active in their role. There were

[42] A *blackhat* is an individual who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2010). Blackhat hackers will be discussed in Chapter 6.

relatively few individuals that met the criteria. The aim was to collect information from frontline experts that were actively working and relevant. The selection of interviewees was a snowball sample (from the meetings that took place that are indicated in Chapter 3.3) and purposively selected (as per the requirements noted in this paragraph).

Employing the grounded theory tradition, the final process involved coding the interviews based on themes, using the same general approach as coding the web forum site content. A difficulty of thematic coding is the tendency to over simplify useful information in the interest of categorising (Boyatzis, 1998, p. 14). Coding was particularly challenging as the discussed content varied greatly among the different interviews. This was expected, as the interviews were fairly unstructured. To address this, all interview data was re-coded a minimum of three times over a period of one year, and then compared to reveal if different themes could be identified. Designing more structured interviews would increase efficiency but this would have conceivably limited the range of discussion by the interviewees. Four of the 12 interviewees offered to provide electronic data relevant to crimeware and botnet activities, which is described in the following section. The presentation of interview data is used to modestly support the findings from the web forum site data and illustrate the themes mainly in Chapter 6. The thesis does not make a claim that generalisations can be made to describe all crimeware web forum sites from the interviews with the 12 participants. It should be reiterated that these 12 participants were difficult to find and are not random computer security professionals. The author surmises there are no more than 100 individuals in Australia that meet the requirements to be included in the study. Refer to Appendix 4 for a copy of the participant information sheet.

3.6 Qualitative Analysis of Electronic Data

The third data source includes a compilation of electronic data acquired from four of the interviews, which are referenced as Case 1, 2, 3, 4 and 5 in this thesis. A list can be found at the beginning of the thesis. The electronic data consists of information generated by, or indirectly linked to, crimeware (see Table 4). Case 1 includes traffic data on different botnet types that are widespread on the Internet, some of which can be directly linked to specific crimeware types. Case 2 and 3 include actual cases of online fraud illustrating the

modus operandi of cybercriminals in which crimeware was used. Both Case 4 and 5 include data generated *in the wild* from cybercriminals that used a popular crimeware tool known as *Zeus.* The use of *Zeus* as a case study is illustrative (it was the only source of data for a specific family of crimeware that could be obtained for the research) and biased. Zeus is simply one example, although considered one of the most prevalent, of crimeware and no generalisations can be made from the analysis of Zeus that extend to all crimeware. Other crimeware tools exist, however data for such other tools could not be obtained for analysis in the research. Case 4 specifically consists of instructions sent by cybercriminals to target particular victims. The *Zeus* crimeware was used to transmit these commands. Case 5 reveals data stolen from compromised computers via a keylogging[43] feature provided as a part of *Zeus*. The date range in which the data was acquired by the interviewees is between 2009 and 2012. The data was received and analysed in late 2012.

Table 4: Breakdown of electronic data

Reference	Data provider	Scale of data	Nature of data	Date collected	Data randomly extracted
Case 1	Non-governmental	Worldwide	Botnet types (statistics)	2011 - 2012	N/A
Case 2, Case 3	Private company	Australia	Phishing[44] and malicious websites (reveals how crimeware is used)	Within 2012	N/A
Case 4	Non-governmental	Worldwide	Commands sent by actors (instructions sent by cybercriminals to target specific victims)	2009 - 2012	100
Case 5	Government	Worldwide	Keylogging data (stolen data from victim computers)	2009 - 2012	100

[43] *Keylogging*, provided through keylogger software, is the act of recording key presses on a keyboard. Such software is often associated with malicious use as it is deployed on a computer without the knowledge of the computer's user.

[44] *Phishing* is a type of email fraud where a cybercriminal attempts to trick a user into revealing personal private information using social engineering techniques. Social engineering involves manipulating people to trust a source, such as an email, using deceptive techniques, for example, posing as a friend, legitimate business or your bank.

Electronic data in the form of data produced by crimeware is a relatively unexplored data source in criminological research. In one part of a broader study on malware markets, Chu, Holt and Ahn (2010) simulated botnet activity and identified that a computer infected as a bot attempted to connect to other systems over the Internet. However, the significance of the traffic was left unexplored. It was evident the systems were impacted and illicit communication may have taken place with other computers on the Internet, yet it was left unexplored as to what the consequences were of an infected bot computer and the contents of such communication. Although likely outside the scope of this seminal and extensive study, an interesting point of investigation could be to examine what is actually taking place. For example, these compromised systems may have been used as proxies to propagate further malicious activities over the Internet or targeted simply for data theft. In this study, the content of electronic data is explored which reveals the intentions of cybercriminals. Actions by botnets may be automated but it must first be directed which requires deliberate human intervention. Such acts are intentional and conceivably derive from some motivation. For example, the keylogging data examined (Case 5), as will be revealed in Chapter 5, include actual instances of bank login credentials being stolen; such data are commonly sold in online web forum sites (Soudijn & Zegers, 2012). This opportunistic behaviour is indicative of monetary gain as a motivation.

The large quantity of electronic data provided a challenge, as it was impractical to examine all the data for Case 4 and 5. To reduce the amount of data to a manageable size, a basic randomisation technique was employed. A randomised sample of 100 cases was extracted from Case 4 and 5 respectively, which were subsequently examined in the study. I should also note that an attempt was made to extract the data using data mining techniques[45] with help from research colleagues.[46] The results of the data mining work are beyond the scope of the research and are not discussed in this thesis.

Criminology research has been somewhat constrained to traditional methodologies (Downes & Rock, 2011, p. 27), which largely include studies based on observation,

[45] *Data mining* is the process of identifying patterns from very large data sets. It draws largely from the fields of computer science and statistics.
[46] This work was undertaken at the ANU Cybercrime Observatory at http://sociology.cass.anu.edu.au/centres/anu-cybercrime

interviews, surveys or the analysis of reported crime statistics. In light of this, an attempt was made early on in the research process to collect primary data directly from the Internet by deploying honeypots using *dionea*.[47] Similar to the investigation by Chu et al. (2010) who monitored botnet activity in a controlled environment, the plan was to capture malicious traffic by purposely creating botnets. However, this approach produced little data and was ineffective.

3.7 Examples to Provide Context

Secondary sources that highlight up-to-date and noteworthy examples of real events that have occurred, largely published from media sources, are provided mainly in Chapter 6. Such examples are provided as context for the relevant themes that are discussed. The secondary sources are merely used to assist in clarifying and illustrating certain themes that are presented. These anecdotal events will be referenced as "Article". A list of these can be found at the beginning of the thesis.

3.8 Ethical Considerations

Ethics approval has been granted for this research in accordance with the National Statement on Ethical Conduct in Human Research (Australia), which was last updated in 2013 (Australian National University Human Ethics protocol number 2011/179). The primary ethical concerns are potential harm towards the researcher, the protection of the identities of observed individuals, and risks related to the nature of the data collected.

The preliminary plan of this research included both a non-participant observation study of online malware communities and a participant observation study engaging with offenders on the Internet. The participant observation part of the study did not take place due to time constraints. A decision was made to carry out the non-participant observation study first chiefly because it was less intrusive and safer for the researcher. In the non-participant

[47] *Dionea* is an open source software based honeypot that captures malicious traffic and payloads over the Internet. http://dionaea.carnivore.it

portion of the study, potential risk to the researcher was minimised, as there was no interaction with the target population under observation.

No deception was used to gain access to the web forum sites. The web forum sites were open and accessible to the public. However, observation was concealed to the observed population in order to reduce risk to the researcher. Such a form of observation could also be referred to as undercover or covert. Additionally, a concern was raised by colleagues of the researcher that publishing the names of the web forum sites would unintentionally encourage inexperienced researchers to visit the sites and become targets of offenders. All names have been kept anonymous and are described in such a way to ensure the identity of the web forum sites and individuals observed are protected. In cases where *vulnerable* targets are mentioned in a discussion post, typically a relatively small website, the names or websites of such targets were redacted. Names and website locations of larger targets, sites that are better capable of securing and protecting their own sites such as a large bank, were not redacted mainly for the reason that they were, at the time of data collection, already listed publicly on the web forum sites.

The interviews elicited in the study were voluntary. All interviewees preferred to have their responses noted down on paper. Electronic recording of the interviews was offered for two of the early interviews, however the interviewees preferred not to be recorded. It should be noted that the two early interviewees did not want to be recorded for the reason that they felt it was safer for them. The decision was made not to offer electronic recording for all subsequent interviews.

The contents of the electronic data raised concerns early on in the research as it contained data on compromised computers. Such data included login and password credentials for certain websites, financial information such as credit card numbers and, in certain cases, contents of personal private messages from different people. It was revealed to the researcher by the data providers that the data acquisition process by the agencies, that collected the data, did not involve illegal activity. For Case 4, the data providers agreed to permit the names of site names to be shown, as they were instructed targets sent by cybercriminals and revealed no details on a target site's vulnerabilities. For Case 5, consent

was obtained from the data providers that publication of the data was allowed under the condition no personal identifiable information on offenders or victims would be disclosed. All electronic data, including data collected from interviews and web forum sites, will be destroyed one year after the completion of the study.[48]

3.9 Addressing Limitations

The previous section outlined some of the ethical issues considered when embarking on the research. In this section, the main limitations of the research are highlighted and the research methodology used including limitations with qualitative research, research design, sampling methods, and data reliability.

Qualitative research is by its nature variable and subjective. The quality of research relies on the capabilities of the individual undertaking the research and their background. It is noted that the researcher had a suitable educational foundation prior to embarking on the thesis with a bachelor's degree in computer science with a focus on computational theory from the University of Toronto, as well as a master's degree in the field of law and sociology from the University of Sydney; both institutions have been ranked in the top three in their respective countries.[49] Since 2001, the researcher has also worked in both governmental and private sector roles (at locations such as South Korea, Australia, Canada and the US) researching as well as developing products to combat online crime. Furthermore, it should be noted that the researcher has had past exposure[50] to online

[48] It should be noted that the ethics guidelines at the sponsoring university for the research (Australian National University) permit data to be stored for up to five years. The data acquired through the ANU Cybercrime Observatory (where the sole researcher is affiliated with) will be stored and held according to the different arrangements made between the Observatory and each third party that has provided data. However, data that was collected for the sole purpose of the PhD research will be destroyed after one year.

[49] Ranks are based on the *World University Rankings 2015-2016* at https://www.timeshighereducation.com

[50] In the 1990s, "hacking" communities prevailed on chat room servers such as on *Undernet* and *DALnet* Internet Relay Chat (IRC) networks. Activities at the time focused on learning to develop software code to impede computer users. Individuals that engaged in such communities would be best described as hobbyists, mostly consisting of people in their youth. It is probable some individuals had ulterior intentions. The motivation of the sole researcher of this thesis, at the time, was primarily aimed to better understand *how computers worked*. Software was a comparatively new technological development in the 1990s and online chat rooms offered one of few sources to

malicious software communities in the late 1990s that could be viewed as a predecessor to the web forum site communities examined in the study. A potential limitation arises as interpretation of data can be affected by bias (Malterud, 2001). Past experiences can affect the interpretation of data and is known as reflexivity, an unavoidable consequence due to "… filters and lenses through which you see the world" (Mansfield, 2006). It is reflexivity that is the greatest obstacle to accurate and impartial results in qualitative research. The researcher's past encounters to similar communities potentially introduces partiality. However, this past experience can also serve as an advantage when interpreting the data, particularly in relation to understanding the nuances and jargon used in web forum discussions. To limit bias in the collection and analysis of the web forum site data, a journal was maintained during the entire process. This journal was subsequently examined to sensitise the researcher of any unconscious subjectivity (for example, changes in life circumstance, increased hours in part-time research work that lead to fatigue, time off taken due to moving homes, traveling and presenting at one conference, relatively important medical issues, etc.), as the full data examination process took place over one year. To address bias in the interviews, a separate journal was maintained to note details of how each interview may have been inadvertently influenced by the researcher. For example, a few of the interviews were confined to within a strict time as the interviewee was busy, and these interview sessions may have been more rushed. Additionally, triangulation[51] was used to validate the interview data, which was done at two levels: the first comparing the meeting of an interviewee with other interviewees, and second comparing the meeting of an interviewee with past meetings involving the same person.

The variable nature of qualitative research also raises concerns of validity or the *richness* of the data examined. To address this issue, the research used a method known as triangulation (Berg & Lune, 2004), in which multiple data sources are examined to support and corroborate findings. Supplementary data sources include interviews with first responders and electronic data. Additionally, there was an effort to select as large a data sample of web

---

acquire knowledge related to programming. Learning to control and manipulate computers sometimes involved creating code, which in certain instances progressed into computer viruses.

[51] *Triangulation* is used in multiple ways in the thesis. Triangulation is used as a technique within the interviews to validate data. Triangulation is also used when presenting 'Zeus' (see Chapter 5 that highlights discussion post content relevant to Zeus, Cases 1-5, and interview comments by Independent #5).

forum sites as possible that could be examined with the limitations of funding and time provided for PhD research. It was a possibility to examine further web forum sites, but this would have potentially led to abandoning the interviews and reduce time to analyse the electronic data, which has been useful for triangulation specifically when examining Zeus. The credibility related to the interpretation of data can also be addressed to an extent as the researcher had past knowledge on similar activities having been exposed to similar online communities in the past.

There are also limitations to the research design and sampling methods. Although an attempt was made to obtain a wide selection of web forum sites, the selection of the sites is fundamentally a convenience sample, and for this reason is not representative of all activities. Additionally, the selection of discussion groups, discussion threads and discussion posts within the website forums are not probabilistic samples. Data was purposefully selected. The quality of relevant data was stressed over the quantity of data.

Data collected within each discussion thread was limited to 10 discussion posts, which may raise concerns, as it is a comparatively small amount. Collecting a relatively small sample of discussion posts per discussion thread limits observation, for example it would be difficult to identify *patterns within* a discussion thread over a longer period of time if only the 10 most recent discussion posts are observed. It should be noted the data was purposefully collected in such a way to capture *as many discussion threads as possible restricting the number of discussion posts under each discussion thread*. An assumption is made that the 10 most recent discussion posts within each discussion thread sufficiently captures online interactions and content.

Another key limitation relates to the reliability of the data in relation to the discussion content on the web forum sites. A possibility exists that individuals involved in discussion activities may capture activities by law enforcement and possibly other academic researchers, which can skew the data (Holt, 2010). However, there is a presumption that such discussion activity coincides with interactions of “real" offenders. Unfortunately, there is no absolute certainty that all the interactions observed exclude such individuals. The research assumes all online interactions and discussions are from genuine members

concerned with the primary interest of the web forum sites. An additional concern is whether the offenders involved in discussions are untruthful. As revealed in Chapter 4.5, in certain cases lying is a common online social practice among members. Dishonesty should be seen as an observed behaviour of online interactions and not as a distortion of the findings.

3.10 Towards a Feasible Model for Offender Resources

This final section continues from the last section of Chapter 2, which discussed the basis of the theoretical framework to explore the concept of offender resources. The research draws from Ekblom and Tilley's paper *Going Equipped* in 2000 and endeavours to expand on Cohen and Felson's (1979) routine activity theory. In brief email correspondence with Paul Ekblom, it was mentioned that the offender resource concept had not been developed further since 2000, when the paper was published, although variations of it have been presented in later publications (Ekblom, 2001; Ekblom, 2005; Wortley & Mazerolle, 2013; Gill, 2005).

In the course of this thesis, a range of criminological theories was considered in conferring with colleagues to identify the best theoretical explanation that recounts cybercrime. Other disciplines were also explored such as education, economics and regulation looking for possible theories. After considering various theories, the routine activity theory was selected as it best described common incidents of cybercrime. However, what is lacking in the routine activity theory approach is the neglect of social factors of criminal behaviour. This thesis endeavours to link social explanations of crime to the routine activity theory. It is acknowledged that no single theory can explain cybercrime in its entirety given its size and diversity rather components of different theories in conjunction can advance our understanding of online criminal behaviour.

Based on a systematic observation of web forums consisting of crimeware related discussions, along with supplementary data sources, my goal is to draw attention to the role of crimeware as a resource used by offenders by relying on established criminological theories, models and postulations to explain offender behaviour. The theoretical

explanations - based on findings in Chapter 4, 5 and 6 - are used as building blocks to consider ways in which to formulate the offender resource concept using the routine activity theory as a guide. The following chapter starts the exploration by examining the online social interactions taking place within the web forum sites.

Chapter 4: Crime Through Association

> The social environment is the breeding ground of criminality; the germ is the criminal, an element which has no importance until the day where it finds the broth which makes it ferment.
>
> *Lacassagne (the "French" Sherlock Holmes)*[52]

The aim of this chapter is to explore the social dynamics occurring amongst the participants of the web forum sites in their natural setting. Using a non-participant observation approach, the content of discussions between participants are analysed. Social learning-based explanations of crime posit that crime arises from the social experience of individuals, an explanation originally used to explain "white-collar crime" (Schlegel & Weisburd, 1994, p. 55) that was first coined by Sutherland (1940). It is suggested that criminal behaviour is learned through interaction with other criminals. This chapter considers the proposition that learning to commit criminal acts involves first joining a criminal or criminal-like subculture (Cloward & Ohlin, 2013), which also necessitates learning the customary behaviours within such collectivities. In such settings, there are certain social processes that can contribute to or hinder the learning process, as will be investigated in this chapter. This chapter will cover four specific areas: an explanation of the fundamental elements of online interaction as it pertains to web forum sites, social dynamics specific to the *novice* or the infrequent visitor, the social norms that contribute to the learning process including those that inhibit such activity, and the relevance of social structures identified within web forum sites interactions.

This chapter explores the findings of the research drawing from Sutherland's differential association theory and, as introduced in Chapter 2, the social learning tradition of explaining crime. The core point of Sutherland's theory, revealed in his 6th postulate,

---

[52] Comment by French criminologist Alexandre Lacassagne translated from "*le milieu social est le bouillon de culture de la criminalité ; le microbe, c'est le criminel, un élément qui n'a d'importance que le jour où il trouve le bouillon qui le fait fermenter*" (Lacassagne, 1913, p. 364). A reader of fictional Sherlock Holmes stories, Lacassagne is referred to by some as the original Sherlock Holmes due to his interest in medicine and crime investigations alike his fictitious counterpart.

suggests that learning criminal behaviour manifests if an individual is exposed to more definitions[53] favourable to criminal behaviour than non-criminal behaviour. In other words, criminal behaviour ensues when there is a surplus of exposure to criminal behaviour, attitudes and motivations compared to non-criminal patterns. As indicated by Sutherland, it is this difference in proportion of definitions that explains the social causes of criminal behaviour, hence the use of the term "differential". This thesis makes the assumption the definitions that favour criminal behaviour are present among the web forum site members studied, however whether such definitions exceed those that favour non-criminal behaviour varies depending on different factors, for example, the amount of time spent on a web forum site or situational context[54] of the offender.

Based on the content of the web forum sites involved in crimeware and associated cybercrime activities, this chapter endeavours to appraise the social learning tradition of explaining criminal behaviour. The broad objective is to advance the theoretical concept of offender resources. The investigation in this chapter will rely mainly on the content of the discussions of the web forum sites.

To recap, the methods in which learning takes place, addressed in the 2nd, 3rd and 8th postulates of Sutherland's theory, which, to summarise, states that criminal behaviour is learned through close interaction among other criminals with the caveat that the processes that entail learning is not exclusive to learning only criminal behaviour. The next section will introduce how learning takes place on web forum sites.

4.1 Nature and Modes of Interactions in Online Communities

[53] Burgess and Akers (1966, pp. 129-130) stated that Sutherland was not clear in how the learning process actually took place. Additionally, Sutherland's reference to the term 'definitions' is also ambiguous. In criminological research, scholars have interpreted this term in different ways.
[54] *Situational context* refers to the surrounding 'online' circumstances of the offender. For example, a web forum site member may only be interested in using botnets. Most interactions surrounding this focus could centre on asking questions related to how to set up botnets, seeking costs to buy botnet access, identifying ways in which botnets can be used to generate money illicitly, or the downloading of botnet kits. Whereas, the situational context of another member could be different as in the case in which an individual is only interested in selling their crimeware tool that may only interact with those seeking to purchase crimeware.

Before examining the discussion content, it is important to recognise the different ways in which interactions take place on the web forum sites. Traditional explanations of interaction within the field of sociology describe social interaction as face-to-face in which there is a "reciprocal influence of individuals upon one another's actions when in one another's immediate physical presence" (Sternberg, 2012). On the other hand, web forum sites allow for interactions to take place in a virtual setting, and it should be noted that such processes are not exclusive to crimeware related interactions. A general web forum site can centre on any subject, forming a virtual community, as well as function as an educational platform.

In the selected web forum sites in the study, members were able to converse in the form of publicly posted messages. Various lines of discussions form "threaded conversations" and can be described as a succession of responses where one person replies to another (Ackland, 2013, p. 65). It is possible for a single discussion thread to contain several discussions that can deviate from the original line of discussion from the original poster [OP].

To highlight an example, in the following discussion thread the [OP] posts a tutorial that describes how to use a specific crimeware tool known as *DarkComet*. The discussion reveals interactions taking place in the form of exchanged messages that are viewable by all members of the web forum site. Online exchanges take place between the [OP] and the different repliers [R1], [R3], [R4], [R6] and [R7]. In the discussion thread, [R1] asks about the purpose of *DarkComet*, and the original poster [R2-OP] subsequently responds with an explanation. In another line of discussion, [R4] states they had trouble with a specific step in the instructions posted in the tutorial. The subsequent response by [R5-OP], who is the [OP], suggests installing software called *proxpn* in order to get the crimeware to work.

> [OP]: I've seen many people using DarkComet more and more nowadays. Therefore, I have decided to make a good tutorial [Tutorial provided]
> [R1]: You are a good person but please what's this for?
> [R2-OP]: It's a remote communication tool to control computers of victims …
> [R3]: Ok bro thanks.

> [R4]: … I not understand part of your instructions, first you enter your no-ip and test your connection but I tested the connection but it's not working. Can you help me?
> [R5-OP]: Install proxpn for port forwarding to verify the test connection …
> [R6]: Hey, I followed step by step your tutorial but I don't know why the connection failed. Ok, I will try again. If I fail again can I ask you for help?
> [R7]: Dude, I don't understand why I need proxpn for this?
> [R8-OP]: proxpn will forward your port so you need this.
> (Forum H2 Thread #2)

There was indication of members contacting other members through communication technologies external to the site. Examples of other technologies used to interact include *Skype*, as revealed in the previous example, and email. Yip (2011) identified *QQ*, a popular Chinese instant messaging service, and its social network features used in underground Chinese carding communities. In the investigation by Holt (2013), web forum sites were used among Russian language members involved in the trade of malware. The difference in technological platforms is noteworthy as language preference may affect the choice of online venue for interaction.

Most interactions were publicly viewable to all members. However, in certain cases communication occurred privately. In the following example, communication starts in the discussion thread, which subsequently continues in the form of private messages, referred to as a "PM", as alluded to in the discussion. Such private exchanges take place between two members and are not viewable by other members. It is evident that further exchanges were taking place outside of what could be observed in the discussion threads. The [OP] makes an inquiry related to the purchase of a virtual private server (VPS)[55]. [R1-A] offers to help the [OP] through *Skype*, and then, as shown in [R3-A], asks to communicate through the private message feature of the site.

> [OP]: Ok, so I recently wanted to buy a VPS from Vortex-VPS, but they said they didn't have any VPS's with Windows. I'm pretty new so I was wondering if anyone could give me any advice to clear things up … Thank you if you take the time to help me …

[55] A *Virtual Private Server* (VPS), which has legitimate purposes, is sometimes used by cybercriminals as a platform to control botnets. It is a service provided by an Internet hosting service provider.

[R1-A]: I will help you bro, send me message with your Skype id.
[R2-OP]: I don't know man. I had to make a new Skype account yesterday …
[R3-A]: Just open your private messages. I will talk with you here.
(Forum A9 Thread #20)

The existence of non-participants of web forum sites that do not actively engage in discussions should also be noted. Commonly referred to as "lurkers", it is believed such individuals achieve their needs, for example the acquisition of information, through observation rather than direct participation (Nonnecke, Preece, Andrews, & Voutour, 2004). Although there is no dyadic exchange or communication, these passive members can still view the discussion threads and its contents. However, it is difficult to assess, or approximate, how many members fall under this category for the observed sites in the study.

The content of both public and private messages were not limited to only text interactions. In certain cases, other information such as website links were provided where software could be downloaded. Website links were typically posted publicly within a discussion thread. In the following example, the [OP] provides a download link of their tool via private messages. The tool is not posted publicly and is only provided to members that respond within the discussion thread, as shown by [R2-OP].

[OP]: Hello fellow members, this is Version 2 of my keylogger with some extra features. Hope you guys will like it … [Screenshot of tool] [List of features of the tool] …
[R1]: Thanks brother for sharing a free keylogger. It's really a nice looking keylogger and I want to use it. Brother, please share a direct link …
[R2-OP]: You are welcome, I PMed [Sent you a private message] you the download link. Have fun.
[R3]: Hey could I have this? It looks amazing.
[R4-OP]: Yes of course you can have it. PMed [Sent you a private message] you the link.
(Forum A4 Thread #19)

Such discussions reveal the direct dissemination of software. Ackland (2013) used the concept of "information public goods" to explain the generation of useful information in

social networks. This view of information is also appropriate to software as it provides value enabling or simplifying a particular action, although this value may vary for different users.[56] Holt and Lampke (2010) investigated carding forums where primarily credit card data was fraudulently traded. More specifically, it was the stolen financial details that were disseminated. In the web forum sites examined, software had been made available in certain interactions. Depending on the discussion thread, software applications, tools and code were circulated for different purposes and uses. For example, the [OP] in the following discussion thread posts two software tools for download that are designed to hack wireless network connections.

> [Topic]: Hack wifi password in windows
> [OP]: … Tool required for hacking
> 1. Commview for Wifi - This tool is used for capturing the packet of wifi …
> [Download link for tool] …
> 2. Aircrack-NG - This tool is used to retrieve password from captured file …
> [Download link for tool] …
> (Forum B1 Thread #2)

Other aspects of interactions also included supplemental visual content such as screenshots (e.g., screenshot capture of a crimeware tool) and YouTube videos (e.g., step-by-step instructions on how to setup or use a specific crimeware tool). Such content in certain cases were posted along with text based information and website links to download software. Communication and online interaction did not only consist of text.

4.2 The Novice, Noobs and Newbies

The social patterns of the new criminal are unique. Sutherland (1956) stated, "… an inclination to steal is not a sufficient explanation of the genesis of the professional thief … [they] must be appreciated by professional thieves (p. 212). A reasonable presumption follows from Sutherland's statement that every criminal was once a *beginner* at some earlier point. Akers and Jensen (2011, p. 248) suggested if criminal behaviour is learned then it follows that there is a variation of actors with different abilities and expertise, with

[56] This notion of 'value' will be discussed in greater detail in Chapter 5.6.

certain actors more specialised than others. As introduced in Chapter 2, Matza (1964) proposed that individuals *drifted* between criminal and non-criminal behaviour depending on the values the individual decides to adhere to and contingent on the degree of socialisation among actors that exhibit criminal behaviour. Matza implied that criminal behaviour should not be viewed as a deterministic state, that is, criminals do not always exhibit criminal inclinations at all times, and that a non-criminal individual can potentially exhibit criminal behaviour. On subcultural views of crime, Cloward and Ohlin (2013) presented the idea of illegitimate opportunities available within a criminal subculture where individuals would decide to engage in illegitimate opportunities if legitimate avenues to achieve success were not available. Cloward and Ohlin's explanation drives the point that interacting with criminals is required at the onset for a potential offender to have the chance to realise such illegitimate opportunities. The basic presumption is that a non-criminal must first engage with criminals before they can acquire and learn criminal behaviours, motivations and techniques.

In the web forum sites, there were discernible activities that revealed interactions relevant to the *novice* offender, for example, individuals with relatively limited knowledge of activities and interactions pertaining to crimeware, botnets and hacking. Among the eight web forum sites investigated, all eight contained discussion groups specifically aimed at new and infrequent members. In an early seminal study of hacker communities by Holt (2007), a causative process is alluded to that starts with an increased interest of technology, which is subsequently followed by a number of other processes namely, yearning of knowledge, commitment to learning, categorisation (simply put, attachment to a particular sub-group or label), and then the role of law.[57]

The following example reveals a discussion thread that is specifically targeted for a beginner audience. In the below case, the [OP] has published a guide for beginners that

[57] Holt (2007) did not present the multiple factors as a 'causal' process rather as normative orders, which do not necessarily take place in any specific order, but this order is implicit. For example, a relationship between the individual and technology (Internet) must exist before the individual can commit to learning technology.

explains how to make money through pay-per-download (PPD)[58] activities. The [OP] claims that they were able to make $50 a day using the guide and charges $15 for the guide. There is a common assumption that criminal communities are generally made up of "expert" offenders, or offenders that have well-established or indoctrinated criminal patterns, however this was not the case in the web forum sites.[59]

> [Topic]: Selling Guide For Beginners
> [OP]: Hey members, I've finished my guide for beginners and I've sold already around 50 copies. I decided to sell 50 more because I've got a lot of PM's from people that want to purchase my guide after I closed my sales thread, so this is your chance! Note, this is the way that I started working with PPD [pay per download] and I'm still having stable income from this method around $50 per day. This month in total I've made $7176.38 and there's still 15 days till the end of the month … Note: This guide is for low to middle earners. With this guide I can guarantee that after 1 month of work you'll see some good earnings! Price for my guide is only, $15. Payment methods: PayPal, Liberty Reserve
> [R1]: I want to buy! Please PM me.
> (Forum E11 Thread #6)

In the case below, a list of websites vulnerable to hacking is offered by the [OP], who indicates that the list of sites may be useful to new users and refers to their target audience as "noobs".[60] By listing vulnerable sites, it has conceivably made it easier for novice users with limited knowledge of cybercrime techniques to engage in malicious activities. Such actions conceivably *prompt* a criminal response (Wortley, 1998), which in this case would involve the "novice" participating in hacking activities, and at the very least facilitate opportunity. It should be noted that there were other discussion threads in which tools and techniques were posted that allowed the *identification* of websites vulnerable to hacking.[61]

[58] *Pay-per-download* (PPD), also known as per-per-install (PPI), is a money-making scheme for bot herders. Bot herders perform the action of installing applications on botnets, or compromised computers, for a fee. Files that are typically installed are usually some form of malicious or unwanted software.
[59] The different types of web forum site members will be covered in Chapter 6.3.
[60] A *noob*, or newb, is jargon that describes an individual that is new to an online community who lacks the knowledge or skills of the specific activity or pursuit of the community.
[61] The process behind the selection of targets by offenders will be discussed further in Chapter 5.5.

> [OP]: Hello … Recently, I have prepared a huge list of SQL vulnerable sites [websites that are susceptible to being hacked], as I had some old lists of SQL vulnerable sites. But most of the links were not working now [the websites are no longer available]. So, I decided to prepare a fresh working list, and it is ready. Hope it will be useful for noobs [new members or infrequent visitors to the web forum site]. Those who want it just post below …
> (Forum A3 Thread #11)

Discussion threads created by new members were usually a form of inquiry or question. The following case shows a request made by a new member who seeks tutorials on the use of bot and remote access trojan[62] crimeware.

> [OP]: Well as you can see I'm kind of new to viruses, just been into bots and RATs. But to be sincere, I know how to create batch file and the simple "viruses" that I know just deletes the boot on windows [preventing a computer from starting up] but nowadays it just asks you for administrator rights [in which obtaining login credentials is the goal] … to get to the point, is there any site tutorial y'all guys can recommend me to read? Can you educate me on writing code that will just mess up a computer? Call me a newb but hey! I gotta start somewhere …
> (Forum D1 Thread #3)

In another example, a new member posts a request to find out which keylogger[63] should be used to steal passwords and asks how it can be operated. [R1] suggests ensuring that the keylogger chosen should be undetectable on a victim's computer, while [R2] advises the [OP] to be careful as the keylogger may inadvertently target their own computer. The web forum sites functioned as a source of information for new members inclined to engage in certain cybercrime activities.

> [Topic]: Working keylogger
> [OP]: So, I want a keylogger that I can send to another person to obtain their passwords. But I'm kind of new to all this, so is there any good working keylogger. How do I use it?

[62] A *remote access trojan*, often referred to as RAT, is a property of software that allows an individual to access and control a system from a remote location. RAT software is commonly associated with cybercrime.
[63] The technical characteristics of keyloggers will be covered in Chapter 5.

> [R1]: Get a simple keylogger then you need to make sure its FUD[64] [undetectable by security and anti-malware products]. I'm not a pro with remote access trojans [referring to keyloggers].
> [R2]: Do not get one off the Internet or you will get keylogged [on your own computer] …
> (Forum D3 Thread #19)

There was also indication that certain discussion content was presented specifically targeted with the "novice" member in mind. As revealed in the topic below, the following example states the tutorial provided is "Noob friendly" denoting that it is easy to follow for inexperienced members. In the discussion thread, the [OP] makes an effort to re-post their tutorial as they accidentally lost their original discussion thread that was created.

> [Topic]: Spy-Net 2.6 Guide To Setting Up and Spreading! … New … Noob friendly
> [OP]: OMG… just OMG … I fucking hate this ... I wrote the tutorial once, and I don't know what happened, I clicked back ... wow… I have to write the tutorial again now, shit ... Okay so lets start again ... fuck. First you need to download these two files:
> [Multiple screenshots provided] [Detail instructions provided] [Download link of tool]
> (Forum A2 Thread #18)

4.3 Basic Elements of Learning

A key criticism of Sutherland's view of learned criminal behaviour is the difficulty to measure and operationalise its theoretical concepts. The field of online learning research discourse provides a useful guide to assess certain aspects of learning in the online environment, which was introduced in Chapter 3.4. In the analysis of the discussion content, there were five fundamental learning processes identified, namely questions and answers, acknowledgement and gratitude, the sharing of information, problem solving, and to some extent imitation was evident. Such elements of learning are not mutually exclusive. Learning can also be viewed as a process instead of an accumulation of knowledge. As a stimuli-response relationship, learning causes an individual to alter subsequent behaviour

[64] *FUD* is an acronym for fully undetectable. It refers to an encrypted file for the purpose of hiding so that it cannot be detected. For example, malicious files that are FUD would not be detectable by anti-malware products. FUD crimeware is an attribute that will be discussed further in Chapter 5.

and this can be long-lasting (Schacter, Gilbert, & Wegner, 2009). The importance of highlighting basic learning processes is to underscore that the web forum sites afford more than a meeting place for arbitrary online dialogue. Examples are included in this section to highlight the fundamental learning processes taking place.

An essential component of learning is making a request to elicit information, which is a basic social process that was evident across all the discussion groups observed. In the next example, the [OP] expresses a desire to start a botnet but is undecided on which type of bot crimeware tool to purchase. The [OP] solicits information on which of two alternatives are best. [R1] insinuates the choice between an "HTTP" and "IRC" bot should be based on what the [OP] intends to do.[65]

> [Topic]: Should I buy a HTTP Bot or IRC Bot? Will be bot herding[66] [creating a botnet].
> [OP]: Well, I'm currently interested in starting a bot shop but, I can't decide which bot to get so, I need some help. What do you guys recommend and, why?
> [R1]: I've had no experience with HTTP bots really, more with some IRC bots, but I've heard HTTP is better for bot herding [easier to create the botnet] and IRC for DDoS [easier for engaging in distributed denial of service attacks].
> [R2]: I'm not sure but I think HTTP bots are easier to use more than IRC [bots], but about the power, I think IRC [bots] are better. Not sure, but you can search on the forums and you'll find your answer.
> (Forum A9 Thread #7)

There was also indication of activity in which members would test and try-out certain crimeware, essentially evaluating the tools to be used for a specific purpose. In the next case the [OP] makes an inquiry about which bot crimeware tool to use to create a botnet of 3,000 compromised computers with the capability to launch DDoS[67] attacks. The [OP]

---

[65] *HTTP* and *IRC* refers to the communication method used in botnet communications. HTTP botnets use website technology as a proxy to communicate, while IRC botnets use chat room based communication protocols to transmit data within a botnet.
[66] There is no official definition of *bot herding*. The act of bot herding generally involves devising ways to create a botnet, in other words compromising as many computers as possible that can be controlled by a cybercriminal.
[67] According to the RCMP, a *DDoS*, or distributed denial of service, attack, "inundate[s] targeted computer servers or websites with false requests until an online service is disrupted and rendered

states that they had previously tried to use versions of *Dirt Jumper*, a specific "brand" of a tool that has the feature to perform DDoS attacks. [R1] recommends two options, and implies that the use of free and cracked[68] tools may have bugs or other problems.

> [Topic]: Need a small HTTP botnet w/ DDoS
> [OP]: I need a small HTTP botnet - 3k bots - w/ DDoS feature. I already tried some botnets like Dirt Jumper v3 and v5, but I'm unable to crypt them [hide them from being detected by Internet security products]. If you know any free ones that are stable, please respond.
> [R1]: You can't crypt Dirt Jumper … try to find one or use YZF/Optima or G-bot. By the way none of the free/cracked ones is perfect though. Good luck.
> (Forum F4 Thread #4)

In certain interactions, members were directed to engage with other offenders to achieve their goals. In the next example, the response to a request by the [OP] was to purchase a crypter[69] to use along with the *DarkComet*. The [OP] was directed to "check the market" which would entail dealing with other members, specifically sellers. It was evident that the web forum sites functioned as a *market* and a source to procure specific crimeware at a cost. This coincides with Holt's (2013) findings in which price was identified as a recurring point of discussion in Russian hacking forums. However, it should be noted that Holt's (2013) formative study concentrated on the view of online forums as marketplaces consisting of buyer and seller exchanges. The scope of this thesis is limited to examining the exchanges that relate to aspects of knowledge transfer, sharing of tools and other learning-specific dynamics, and thus an in depth examination of themes dealing with interactions of a transactional buyer-seller nature may be limited. Additionally, whether there are any differences due to the English language focus of this study is unclear. The example reveals that some minimal level of interaction may be necessary, as members would have to deal with sellers, distributors and providers of crimeware to obtain what they need. Interestingly, [R7] suggests to the [OP] to make an effort to build their own crypter.

---

inoperable, which may in turn prevent legitimate consumers from using the targeted service" (RCMP, n.d.).

[68] *Cracked* software will be covered in Chapter 5. Simply put, cracked software refers to software that has been modified in a manner to circumvent technical measures to protect such software from being used by unregistered users, specifically users that have not paid for the software.

[69] *Crypter* is a category of crimeware tool that will be covered in Chapter 5. Crypters allow files to be obfuscated to prevent them from being detected by Internet security and anti-malware products.

[Topic]: DarkComet RAT Help me please
[OP]: So I am using DarkComet and it's awesome, but I need a crypter so it will crypt everything in a exe file [the malicious files that are spread to victim computers] so that anti-virus [products] can't detect it. Thanks for the help, my friend and I have looked everywhere for a good free one but have had no luck.
[R1]: Don't waste your time with free crypters. You can buy a crypter, usually a limited-time license, at a cheap price, check the market. Beware of offers that just look too good, their feedback system works on the border of scam.
[R7]: You could attempt to encrypt the file yourself, or just purchase a crypter from some "hacking" forums.

Acknowledgement by repliers in the form of gratitude was also common behaviour. It appeared that gratitude was provided typically if the discussion thread, posted by the [OP], was deemed as useful. In the following example, various repliers acknowledge the post by the [OP] as helpful.

[OP]: [Free] Dracula Logger Public | FUD 0/37 | 12 Stealers[70] | Perfect for beginners, [Screenshots of tool provided]
Features: Fully undetected, I may drop in every once in a while to clean up the detections. Currently FUD as of 9/18/2012), Custom Installation/Startup Path, Icon Changer, …
[Download link of tool] …
[R1]: Nice share bro keep it up.
[R2-OP]: Thank you mate.
[R3]: Thanks a lot bro really appreciate it.
[R4]: Nice share I'll have to try it.
[R5-OP]: You're welcome mate.
[R6]: Too good. Thanks mate.
[R7-OP]: Your welcome bro.
(Forum H4 Thread #18)

In the following example, the [OP] explicitly asks for gratitude using the site's feature that allows for reputation to be accrued and viewed by other members.[71] Interestingly, Forum A

[70] *Stealers* are a type of keylogger that is found on a victim's computer that aims to capture data, and then transmit it to a cybercriminal.
[71] Trust and reputation have intrinsic 'value' among web forum site members. It is an element that can be 'accumulated', which will be discussed further in Chapter 5.6.

and C provided a “thanks” and “rep” (reputation) button that could be selected by repliers. These features were not available on the other web forum sites.

> [Topic]: Earn 80$ daily private, now public
> [OP]: Hello … members, I'm posting here great method to earn more than 80$ daily. If anyone needs the method, PM. Will send it to you when I'm online. Rep and thanks.
> (Forum C4 Thread #4)

Sharing, through the free distribution of crimeware tools, is another common behaviour that was identified. In the following two examples, crimeware tools are *given out* that were not originally created by the [OP]. Such activity increased the availability of certain crimeware tools as they were openly accessible for download with no fee required. *DarkComet* is provided free for download in the first example, and *Cybergate* is made available in the second case. Such instances illustrate that certain crimeware tools are circulated free of cost, which demonstrates that web forum sites do not always consist of buyer and seller exchanges.

> [Topic]: DarkComet 5.3.1
> [OP]: So you must be thinking why there is yet another thread for this free RAT [remote access trojan]. Well here is the reason. If you didn't know, the author of DarkComet has stopped updating or renewing the RAT anymore and he won't be continuing the RAT project sadly. So here is the latest version that was out just in case you were not able to get it. It's a direct download link, so enjoy: [Download link for tool]
> [R1]: Thanks so much for this. You are a boss. Sharing is caring, and you CARE!
> [R2-OP]: You're welcome. Thanks for the comment.
> (Forum H4 Thread #10)

> [Topic]: Cybergate V1.07.5 Download Link
> [OP]: As I was checking the Internet I realised that it is really difficult to find Cybergate V1.07.5 download link that is working so I decided to share it here so that it can be easily downloaded [Screenshot of tool] [Download link of tool]
> (Forum H4 Thread #6)

Interactions also indicate problem-solving occurring in certain discussion threads. In the following example, the [OP] states they have had difficulty setting up *DarkComet*. The

repliers [R2] and [R3] recommend solutions to resolve the problem of the [OP]. With the evaluation of different solutions, such interactions reveal multiple members working together to solve technical issues associated with crimeware.

> [Topic]: DarkComet RAT Help me please
> [OP]: First I would like to say hello to the forums but what my problem is I have been trying to set up DarkComet RAT. I have been having nightmarish problems and I could really use some help cause I've been trying to forward my ports but its saying it can't, all very frustrating. I was hoping someone would be kind enough to help me out over Team Viewer 6 [help via remote desktop sharing]. I would be in a world of debt and greatly appreciative … please someone help me out here I've been wracking my brain over this the past few days.
> [R2]: Use some vpn with open ports or first install the bittorrent or utorrent then note down the ports …
> [R3]: Dude, make sure you forward ports correctly also to add DarkComet as a firewall exception. If you getting error again, pm me and I will set it up …
> (Forum E8 Thread #19)

In another case, one replier [R1] suggests to the [OP] to contact the support team of *Blackshades*,[72] a remote access trojan that was prevalent among the web forum sites at the time of data collection.

> [Topic]: Blackshades Weird Error
> [OP]: Well I'm using Blackshades 4.2 and while creating the server I got this weird error! The problem is that I couldn't find anything for it even on google! [Screenshot of problem] Any help on this would be appreciated! Thanks in advance!
> [R1]: You should contact the support for Blackshades.
> (Forum E8 Thread #10)

A form of imitation could also be inferred in some instances. The following example reveals the act of creating crimeware tools being emulated. The replier [R1] praises the [OP] for being able to create their own tool who implies that the [OP] was unable to do so previously. The [OP] has conceivably progressed from initially having to acquire crimeware from other members to creating their own. The response by [R1] could also be

[72] In *Operation Cardshop* in 2014, the FBI arrested a cybercrime gang responsible for *Blackshades* (FBI, 2014). The primary point of distribution of the Blackshades remote access trojan (RAT) crimeware tool was web forum sites.

interpreted as a compliment to the [OP]. As will be highlighted in the next section, Chapter 4.4, encouraging comments may compel and drive certain behaviours.

> [OP]: Illusi0n | SkyeCrypter [Download link of tool]
> [R1]: Few hours ago you wanted my crypter tool, now you created your own. Nice, vouch.[73]
> (Forum G3 Thread #5)

4.4 Learning Contributors

Burgess and Akers (1966) posited that certain behaviours among offenders were rewarded, while unwanted behaviours either went unnoticed or was criticised. The belief was that certain behaviours were strengthened based on past actions and experiences, and in the case of actors involved in crime, comprised mainly of behaviours considered favourable among criminals. The consequence of such a theory would mean that offenders as a social system would have a propensity to self-perpetuate, thus continually nurturing and promoting further criminal behaviour. Moreover, Burgess and Akers (1966) presumed that the potential offender would need to be indoctrinated into crime, before certain behaviours could be reinforced. As revealed in Chapter 4.2, it was shown that certain web forum site members that participated in discussions were new or infrequent visitors. If certain behaviours were sufficiently reinforced among such members, the effect may lead the *novice* to engage in further criminal behaviour and potentially escalate to other forms of cybercrime.

Social processes were evident that contributed to the learning of certain behaviours, values and skills. In the web forum sites, such processes are manifest in four different ways, namely as online interactions that supported certain behaviours, the elicitation of feedback, guidance from "experts", and the influence of trust and reputation when learning.

Certain web forum site interactions showed that gratitude expressed among web forum site members has a role in influencing subsequent behaviour. In Chapter 4.3, the previous

[73] A *vouch*, or the earning of a vouch, is one way in which positive reputation can be developed. Chapter 4.4 and Chapter 5.6 will examine these interactions in more detail.

section, it was observed that gratitude was directed towards a member in situations if the member made a post that provided a valued tool. There was indication that certain behaviours such as creating discussion threads on useful tutorials were rewarded through postings that expressed appreciation. In the following example, gratitude is directed to the [OP] who posts a tutorial on a Java botnet. Such actions reward and encourage the [OP], which conceivably encourages the [OP] to repeat such activities.

> [Topic]: Java Botnet tutorial
> [OP]: This is one I wrote for [this site]: Ok, first off you need an IRC channel - two helps! - and you need to have java JDK [programming language environment] installed on your computer. Now this usually comes with most computers now.
> [Tutorial is displayed]
> [R1]: … I thank thee ... One up for you.
> [R4]: Thanks man, keep the good work up!
> [R5]: Very useful thanks
> [R6]: Thx man I like this source
> [R7]: Nice and thx this source
> (Forum E5 Thread #17)

Another element of learning involves the elicitation of feedback. The outcome of feedback is assessment that may be used to improve or maximise the utility of a discussion thread. The [OP] in the following example creates a discussion thread related to a tutorial on "HTTP botnets". The key point of interest is at the end of the post in which the [OP] explicitly asks other members to post comments if they have any concerns with the tutorial.

> [Topic]: HTTP botnet Tutorial (noob Pr00f)
> [OP]: As many of you might have noticed this week … I have been working around HTTP botnets and I finally came across one that is sort of easy to set up and learn from. And have made a botnet, so I thought I will spread the knowledge. Things you will need … Comment if you have doubts …
> (Forum E5 Thread #14)

Similarly, the [OP] in the next example invites "suggestions and feedback" in their tutorial that outlines how to hack email accounts.

> [Topic]: How to hack e-mail accounts, A Detailed Tutorial!

> [OP]: The Internets most asked question of all time! How can I hack hotmail/gmail/yahoo/facebook … I hope this sheds some light and answers on the most asked question of all time. Feel free to add your suggestions and feedback. [Tutorial provided]
> (Forum E3 Thread #15)

As in the previous two examples, the [OP] in the next example asks for feedback and makes a request about whether mistakes were found, in other words seeking criticism, on the tutorial that they have posted.

> [Topic]: What is difference between persistent and non-persistent XSS? [a hacking technique to attack websites]
> [OP]: Hello … Here's a great tutorial for people who are learning XSS attack [Tutorial provided]
> [R1]: Very nice and well written.
> [R2-OP]: Thank you … If you or anyone else has a question about the topic then don't be afraid to ask. Also if there was a mistake then please [reply to discussion thread] … even if there is a little grammar mistake.
> (Forum H3 Thread #14)

Additionally, discussion threads that provided crimeware tools for download in certain cases offered supplemental direction and guidance. For example, the [OP] in the subsequent discussion thread advises other members to use the tools in a sandboxed[74] environment, in addition to making available a selection of hacking tools for download. Such advice helps to protect web forum site members from imprudently infecting their own computer with crimeware. It should be underlined that this additional information was provided voluntarily by the [OP].

> [OP]: Hack Pack! 33 Hacking Tools
> Keylogger and password stealing: Ardamax 2.8 / Ardamax 3.
> [Other tools listed for download] …
> It would be best to run all these tools either Sandboxed, or from a Virtual Machine …
> (Forum B1 Thread #11)

[74] *Sandbox*, or sandboxing, is a technique used in the field of computer security to run untested programs or malware in a separate isolated environment. It is done to prevent such software from adversely affecting a user's computer.

Trust also played a role in learning certain behaviours. Von Lampe and Johansen (2004) suggested that trust is often used in studies related to organised crime, which is explored as an important dynamic to explain how individuals cooperate. Emphasising the significance of trust among criminals, Gambetta (2009) stated that reputation played a more crucial role among criminal populations than in non-crime related interactions and settings. When describing online actors, Lusthaus (2012) suggested that a large barrier for cybercriminals to develop trust was due to anonymity, and to establish trust the cybercriminal would need to cultivate their online identity. The research by Holt (2013) also identified trust as a key social dynamic in publicly accessible Russian web forums involved in malware activities.

Through an investigation of botnet forums, Décary-Hétu and Dupont (2012) suggested that peer reputation systems, structures built as a part of web forum sites, helped members on the site to distinguish which members were more reliable. Actors that were involved in *more* positive interactions, and successful dealings, were more likely to be perceived to be trustworthy. In a study on reputation systems of *legitimate* online auction sites *Ebay* and *Taobao* (the Chinese equivalent of Ebay), Ye, Xu, Kiang, Wu and Sun (2013) identified that having a greater positive reputation granted benefits for sellers such as the listing of items for sale at higher prices.

In the web forum sites, it is evident reputation systems not only provided the function of identifying reliable members, but also to influence and drive certain behaviours. Gathering reputation "points" appeared to encourage participation, in a manner acting as a form of reinforcement. In certain discussion threads, there were cases of members specifically asking for a “thanks” or “rep”, available as buttons on the web forum sites that included such a feature. The clicking of such a button was a means to show approval, as highlighted in Chapter 4.3. It may also be a reason behind certain actions if maximising trust, or one’s reputation, is considered favourable. Sites such as *Stack Overflow*, an online question and answer website platform that caters to programmers, provides a “bounty” system in which participants can “slice off” their own reputation and offer it to others that answer their question (Stack Overflow, n.d.).[75] The bounties are used as a type of currency to encourage

[75] *Stack Overflow* is an online question and answer platform, which shares similarities to discussion forums (the web forum sites examined in this research).

people to answer questions. The web forum sites examined in this research did not include such a system of *transferring* reputation. However, there was indication that web forum site members created discussion threads with the goal to accrue reputation.[76]

In the following example, [R4] tells the [OP] that no one would trust them as they have not participated enough in the web forum site.[77] Such interactions suggest that the *novice* or members with an insufficient number of discussion posts are perceived to be unpredictable.

> [Topic]: Tornado Crypter …
> [OP]: First of all, sorry for my bad English. So here is my first crypter ... [Details of tool] … Download: I await your comments before posting the download link.
> [R4]: … you have 24 posts, people will not trust you …
> (Forum G3 Thread #7)

Certain members had negative reputation points, specifically in the case of Forum A. In the below example, [R2] suggests not to follow the advice of another member [R1] as they had a negative reputation score.

> [Topic]: How to hack a Facebook Account?
> [OP]: Does anyone have a tutorial on how to hack a Facebook account on a mac?
> [R1]: Get jRat, it's a remote administration tool that allows you to control the person's computer. Once you have that you can access anything you want including email, facebook, gmail …
> [R2]: I wouldn't suggest following the advice of the alpha [referring to R1] with -5 rep, because it is extremely easy to trace the IP [if using jRat].
> (Forum A1 Thread #16)

Trust could be established in alternative ways. As pointed out in Chapter 4.3, the act of "vouching" a member was a way to express that a particular member had a successful exchange. By posting such a statement, it indicates to other members that future dealings with the member has a greater chance of a positive experience. The reputation system (the "thanks" and "rep" button) and "vouching" appear to be used in similar situations, however

[76] This notion of reputation as a form of value among offenders will be covered in Chapter 5.6.
[77] In the web forum sites examined, the number of posts made by a member since their registration date (when they first joined the site) was shown next to their name.

"vouching" is considered a more public expression, requiring a discussion post, whereas clicking the "thank" or "rep" button simply adds to a member's reputation score. In the following example, [R6] vouches *in the open* for the [OP] who has posted a JDB[78] (java drive-by) exploit.

> [OP]: Hey … Today I release my private JDB [java drive by download] … to the public. To get it you must post here and pm me …
> [R6]: Vouch for this user, 100% legit as fuck, you can deal with him.
> (Forum A4 Thread #13)

Proving trustworthiness was important in discussion threads that involved the selling of cybercrime products and services. The [OP] in the following example has posted a list of customers that has had positive experiences with them. Such "vouches" had to be purposefully gathered, which likely involved multiple exchanges and ensuring those transactions were positive for the buyers. Such patterns concur with Holt's (2013) findings in underground forums where customer service was a common theme that was pointed out. Recording positive interactions are an indicator that customer service is considered important. It is conceivable that the forces that drive learning processes are a by-product of building trust and reputation.

> [OP]: …
> 03-14-2012 09:25 PM – [Username redacted] Wrote: Bought services from him on the 193k page. Got a lot of likes and views.
> 03-14-2012 03:28 AM – [Username redacted] Wrote: Vouching. Bought and he did as requested!
> 03-13-2012 10:50 AM – [Username redacted] Wrote: Vouch for Glomerulus! Legit seller bought some stuff from him.
> 03-12-2012 08:41 PM – [Username redacted] Wrote: Had his service before and I must vouch
> 03-10-2012 09:38 PM – [Username redacted] Wrote: Legit user and product thanks alot bro beans
> (Forum A13 Thread #6)

[78] *JDB*, or java drive-by, is exploit code and a technique used by cybercriminals that involves tricking a victim into downloading software with the goal to compromise their computer. The victim accidentally downloads the malicious file, which appears to be innocuous.

Interactions that reveal having a strong reputation being a positive characteristic supports the claim that being perceived as trustworthy plays a beneficial role in the success of future dealings. As Holt, Strumsky, Smirnova and Kilger (2012) identified in their social network study of Russian hackers, individuals situated in denser networks (individuals with a relatively high number of "friends" that can imply having a strong reputation) have considerable impact in contributing to cybercrime. Also, such a social structure indicates a hub and spoke organisation (McGuire, 2012).

4.5 Learning Detractors

Von Lampe and Johansen (2004) suggested that the consequences of breaching trust among offenders can vary and that in certain cases there may be no outcomes of such acts. On the web forum sites, there were cases of trust violation in which members would publicly denounce other members. The showing of disapproval publicly, through posted messages, was used to indirectly communicate to other members that a particular member could not be trusted. In addition to the social dynamics identified that contributed to learning certain behaviours among web forum site members, social processes were found that worked against the learning process. Such interactions should not be viewed as an opposing contradictory social dynamic to the sharing of knowledge or tools but one part of the broader learning process among web forum site members. There were three themes that arose, namely deception towards web forum site members, declaration of dissatisfaction of certain actions, and barriers to participate in certain activities.

The first theme involves instances of deception observed on the web forum sites. It is important to clarify that there are two different directions in which deception can occur. Forms of deception may be used between members of the web forum sites, that is, one web forum site member may target another member. It can also be directed towards non-members, or the targets of cybercrime, that are external to the web forum site. The former is the point of focus in this section, and the latter theme will be discussed in Chapter 5.

The next three examples reveal members that targeted other members by distributing backdoored[79] crimeware tools. There may be a greater risk of victimisation within the web forum site population simply for the reason that members, being potential victims, participate and engage in a community associated with precarious activities (Lauritsen, Laub & Sampson, 1992). Such software would attempt to perform unwanted actions on the computers of the users of the crimeware tools. The first example reveals the reserved suspicions by certain members of a tool distributed that steals access to already compromised computers. In the second example, the replier [R5] notes the possibility that the remote access trojan known as *XtremeRAT v3.6* provided for download may be backdoored, but states they accept the risk of using it. The third example reveals a comment by [R4] that the *Limitless Keylogger* provided was tested and confirmed to be backdoored, consequently warning other members.

> [Topic]: Team indishell cpanel cracker
> [OP]: [Download link of tool] [Screenshot of tool]
> [R2-A]: Nice tool, thanks for sharing but I am afraid it might have a backdoor that steals shells[80] or cPanels [botnet command and control sites]. Just saying.
> [R6]: Beware ... this code seems have signs of a backdoor to me … it's mailing someone it seems!
> [R7-A]: Lol, not that I don't like the post but I'm just saying, it may be backdoored.
> (Forum C4 Thread #8)

> [Topic]: XtremeRAT v3.6 private and Spanish
> [OP]: Hello friends here I leave this mouse [remote access trojan] for those who do not have one ... I added some skins to search the web [added a search feature] ...
> [R1]: Hope you're not trying to infect members?
> [R2]: Friend, I'm not trying to infect anyone ... I'm just bringing it here … I got the program from another forum ... I just added the skin
> [R5]: Thanks, I'm going to try it - and hoping that it's not backdoored
> (Forum C9 Thread #11)

[79] A *backdoor* refers to crimeware that deceptively aims to target the user of the crimeware. For example, a computer on which a backdoored crimeware tool is being operated would be accessible to another person without the knowledge of the computer's owner. Simply put, the offender is the targeted victim. A common occurrence on web forum sites is to distribute backdoored crimeware with the goal to take control of botnets controlled by other web forum site members.

[80] A *shell* is a form of crimeware that allows the cybercriminal to access and modify files on a targeted server or computer over the Internet. Crimeware tools will be covered in greater detail in Chapter 5.

[Topic]: Limitless Keylogger [cracked]
[OP]: This is one of the advanced Loggers/Stealers/RATs around the web. It has tons and tons of features.
[R1]: Any feedback about this keylogger?
[R2]: Don't download ... backdoored.
[R4]: Tested and its backdoored, don't download.
[R7]: Hope it is not backdoored. I will try.
[R8]: Backdoored.
(Forum G3 Thread #17)

It was clear certain members had nefarious intentions towards other members. The [OP] in the following example has posted a dork[81] tool, with likely dishonest intentions, that is aimed to target members that download and use the tool. Interestingly, [R4] threatens to report the activity to the web forum site administrator. Such interactions show that members were able to report problems to an admin, which may involve the punishment of undesirable behaviour. The type of punishment that would be applied to such behaviour is not clearly revealed, however the presumption is that it involves the banning of the individual's account.

[Topic]: Dork Scanner New … updated with the latest dorks … Hack shops easily!
…
[OP]: Here is a tool from me, this scans all dorks for SQL exploit
[Download link of tool] [Websites vulnerable to injection attacks]
[R1]: This is a virus.
[R2]: Why you do want to infect members?
[R3]: What the fuck has this to do with infecting members. The file is clean. Go scan it!
[R4]: Ok, here is the result. My antivirus is blocking the download. So, there is no doubt that this is infected. Post virus scan and a screenshot. Otherwise I'll report this.
(Forum C6 Thread #20)

The second theme, criticism between web forum sites members was also evident in the discussion threads. Certain behaviours were condemned, or a member blamed, if certain actions did not provide benefit to a member or the larger web forum site community. In the

[81] A *dork* is a technique used by cybercriminals to identify vulnerable computers, servers and websites on the Internet using Google search queries. Dorking will be covered in Chapter 5.5.

following example, [R1] disapproves of the $50 cost of the *Blackshades* remote access trojan for sale by the [OP]. Additionally, [R2] states that the crimeware tool is obsolete. The posting of tools that were out of date, or were priced too high, was questioned.

> [Topic]: Blackshades NET 3.4
> [OP]: Deciding between a RAT, a host [booter],[82] or controlling a botnet has never been easier. With Blackshades NET, you get the best of all three [Technical description of tool] The price is a light, one time fee which includes all updates of the program. Price: $50 …
> [R1]: You sell at a very high price.
> [R2]: Outdated but thanks.
> (Forum C6 Thread #6)

Condemnation occurred if a crimeware tool was unable to avoid detection and failed to perform its intended function.[83] The following example shows a replier [R1] expressing disapproval of a keylogger tool called *Ardamax* as anti-malware products were able to detect it. The detection of such crimeware would render it unusable.

> [Topic]: Ardamax keylogger v3.0
> [OP]: Download: [Download link of tool]
> [R1]: Me personally don't like Ardamax because it's detectable by most anti virus.
> (Forum E10 Thread #2)

The third theme involves barriers to participate in certain activities. There were some notable differences between the web forum sites in the study. For example, one web forum site provided labels for its members. Forum A had specific designations for its members, resonant of a kind of social stratification; "staff" was the highest followed by "uber", next was "elite", and finally "epic". Interestingly, in one case the [OP] provided their tutorial to higher-level members first along with a requirement that a minimum number of discussion posts be made. Such factors conceivably act as an obstacle to access particular content, particularly for the *novice*. Web forum site members that actively responded to discussion threads, posted tutorials or distributed crimeware tools achieved a higher-level label, as the higher-level labels appeared to correlate with members that posted more regularly.

[82] A *host booter*, or booter, is a crimeware tool that performs the function of a DDoS-type attack.
[83] The features and functions of crimeware will be covered in Chapter 5.

Interestingly, the other seven web forum sites examined in the study did not have such labels.

> [OP]: Hey guys! … I'm giving away my Tutorials collection …
> I have added some rules: You will only get it when you have at least 2 Stars - 50 posts I think - So I don't waste my time. I send it first to … [uber], [elite] and then [epic]. Thanks for understanding :)
> (Forum A3 Thread #17)

The previous example reveals that a social structure may exist on certain web forum sites to separate members based on their level of participation.

For illustrative purposes, details from Forum A are shown below that show instructions on upgrading account labels. Note that accounts are "manually reviewed and required to meet certain criteria" before it is upgraded, in addition to the required fees.

> Upgrading … This is the FAQ about account upgrades.
> How much does it cost to upgrade? Currently there are three options for paid membership:
> 3P1C [epic] = $15
> L33t [elite] = $18
> Ub3r [uber] = $25
> What benefits are there for upgraded accounts? - Read the upgrade page. There might additional benefits not listed.
> How do I know if I qualify to be in the ub3r group? - You can start the process on the Ub3r Application page.
> Why do you require approval for Ub3r? - This is our highest level paid group. Each account is manually reviewed and required to meet certain criteria to be approved. We do this in order to ensure the best integrity possible for the group.
> If I am denied, can I reapply? - Yes you can, but only after 60 days have passed. Be aware you may be permanently denied ub3r if an account review reveals that you're a low quality user.
> I was denied ub3r. Can I find out why? - No, you cannot. We do not publish requirements thus we can't provide you denial reasons. Do not PM admins inquiring about denial reasons.
> I paid for membership, how long till my account is upgraded? - Typically within 24 hours. Do not inquire via PM or create a support thread until at least 24 hours have

passed. Include your transaction ID. If you paid with your Paypal and it was an echeck, it can take 5-7 days to clear.
(Forum A)

The following section will discuss the significance of social groups in more depth among the web forum sites.

4.6 The Relevance of Social Structures and Organisation

There continues to be a deficit of empirical research on the social structures and operational characteristics of the organisation of cybercrime offenders. Wall (2014) noted that little is actually known about the organisation of cybercriminals. It was Brenner (2002) who suggested that it was the differences in the terrestrial and virtual world that made it difficult to apply terrestrial explanations of criminal organisations to the Internet. In spite of this, it is clear that known cases of offenders, largely those arrested by law enforcement, have been used to generate speculative models on the organisation of cybercrime (Broadhurst et al., 2013).

McGuire (2012) proposed three broad typologies of groups involved in cybercrime activities, namely groups as swarms that are reminiscent of larger disorganised collectives, groups that traverse the Internet and extend into the offline environment, and hierarchies. The focus of McGuire's approach was on the structures and connections between individuals and groups. The general argument from McGuire's study was that the organisation of cybercrime gangs could take on a form different from the stereotypical hierarchical structure associated with the customary view of organised crime. In contrast, Chabinsky's (2010) view of the criminal organisation in the cybercrime setting focused on the function of individuals that are involved in specialised roles.[84] For example, in the sophisticated cybercrime ring there are different roles such as malware authors and money mules, who work together, that are required for an online fraud to succeed. It was the

[84] It should be noted that comments made in the FBI report (http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom), which was originally notes for a speech, by Chabinsky is potentially based on the *DarkMarket* cybercrime forum that was infiltrated by the FBI in 2008. It is likely Chabinsky's account was intended to be an observation of how *DarkMarket* operated, and not meant to be an explanatory model to depict organised crime on the Internet.

functions of actors rather than linkages between actors that were the emphasis, in comparison to McGuire's classification. In the web forum sites, three themes arose which pointed to the existence that some form of organisation was manifest among the web forum site members, namely the collaborative nature of interactions, indications and references to the existence of groups, and the maintenance of order of the larger web forum site community.

The first theme involves the collaborative nature of interactions. From the field of organisation science, Zollo and Winter (2002) described three basic methods in which learning took place within an organisation; these include learning by action (performing the act), the dispersal of knowledge (knowledge creation), and the storing of knowledge (as cited in Ayling, 2009, p. 192). Each of these points is certainly observable on the web forum sites. It would follow that web forum sites are a form of organisation, if all that were required were the three conditions to be met. The prerequisite for any sort of organisation is interaction of individuals, or at least three persons according to Article 2(a) in the definition of the "organized criminal group" by the *United Nations Convention on Transnational Organized Crime* (UNTOC, 2004). Additionally, collaboration involves the act of multiple individuals coming together for a specific goal. The web forum sites, as shown in previous examples, clearly indicate multiple users were interacting for reasons typically linked to the goal of the OP of the discussion thread.

In most discussion threads it was evident that multiple users communicated on specific points of inquiry. The [OP] in the following example has created a discussion thread intended to invite ideas of different members on social engineering techniques.[85]

> [Topic]: Ultimate Spearphishing
> [OP]: Okay so this guide is intended to be a collaboration between users, and continually updated with new ideas on social engineering. Step 1: …
> (Forum D4 Thread #4)

[85] *Social engineering* involves the use of deception to elicit information from a victim. Social engineering attempts to build a false sense of trust with the victim, and then takes advantage of this relationship to obtain information (Chantler & Broadhurst, 2006).

In another case, collaboration involved the exchange of software code and the use of servers between members. In the following example, a tutorial is provided on how to engage in DoS[86] attacks through a virtual private server (VPS). In the discussion thread, the [OP] thanks two members, one who provided the code for the DoS attack and another member that offered the use of a VPS as a test platform.

> [OP]: Hello … I haven't seen a legitimate tutorial on how to use a VPS to send DoS Commands through an SSH Client with a perl script [crimeware], so I decided to make a tutorial for those who are curious.
> [Tutorial provided]
> Credits: I wrote this tutorial 100% by my self, the perl script [code used to engage in the DoS attack] provided was made by [Username redacted].
> Special thanks to [Username redacted] for providing me with a VPS to use …
> (Forum A2 Thread #11)

The creation of crimeware tools in certain cases was not a solo pursuit. The following example is a clear case of a tool called *Lost Door v8.0 Pure* developed with the assistance of multiple individuals. For instance, certain members assisted in testing the tool, while other members helped to develop the visual graphical layout used in the tool. This example would be consistent with Chabinsky's model of criminal actors that have specialised functions.

> [Topic]: Lost Door v8.0 Pure - Released 16-10- 2012
> [OP]: Special thanks for [Username redacted] for being the reason to create this tool in 2007
> Big thanks to [Username redacted] for keeping Lost Door up by his tests & idea since 2008
> Thanks to all the beta testers & friends: [Usernames redacted] etc. Thanks goes to [Username redacted] for his codes share & to [Username redacted] for the graphics help. Thanks goes to the following website [Site names redacted]
> (Forum C9 Thread #22)

[86] *DoS*, or denial of service, attack is a specific form of a DDoS attack in which only a single computer is involved in "flooding" the connection of the victim computer or server.

In certain cases, it was evident that to perform DDoS attacks, that knowing or having access to the right actors helped. In the follow example, [R1] states that eliciting botnet services, through other members, is a possible means to engage in DDoS activities.

> [Topic]: Best way to DDOS other then a botnet?
> [OP]: Any services I can pay for? Really can't be bothered setting up a botnet and try spreading it, everyone's doing it.
> [R1]: It's relatively easy to perform DDoS attacks. If you don't want to make a botnet then you have to purchase or rent one from someone, but that costs a lot unless you know the right people.
> (Forum H1 Thread #27)

The second theme involves evidence of the existence of closely-knit groups. The [OP] in the following example asks whether "clans" exists in present day. Interestingly, [R1] implies that a way to join such groups would be to build "quality exploits" as a means to gain entry. Additionally, [R3] mentions there has been a growth of "sec" groups since the prominence of *LulzSec*,[87] a widely publicised hacker group that has been associated with *Anonymous*.[88] It should be noted that it was not possible to observe the interactions occurring within such groups on the web forum sites.

> [Topic]: Are there any hacker clans still around?
> [OP]: I've been wondering if there are any hacker clans still around? This question is directed more at the new era, not much of the old era of hacker clans. It's also a thought from my mind if the hacker clans engage in wargames and skill building activities, or just deface websites randomly.
> [R1]: Yes, write some quality exploits, keep them to yourself, use them, trade them with others … and you'll find them.
> [R3]: Clans? Anyway, yes of course. Have you not noticed all the *sec groups that have come around since LulzSec? Skill building and wargames is more for the whitehat communities. You don't need a closed circle for that.
> (Forum D1 Thread #2)

[87] *LulzSec* is a computer hacker group known to be involved in a series of high profile cyber attacks, one of which includes the Sony Pictures breach in 2011. The group is rumoured to have disbanded in 2011 (Brown, 2011).
[88] *Anonymous* is a large community of "hacktivists" associated with ideologically motivated cyber-attacks.

Lacking the appropriate expertise provided a barrier when engaging with certain offenders. The following example suggests that insufficient ability may hinder individuals from joining a group. [R1] indicates that to join a group that a potential member must have the proper skills, and implies that "noobs" would have difficulty entering such groups.

> [Topic]: Help joining a clan!
> [OP]: Hello, I am fairly new here and I want to learn as fast as I can. I have heard that there are clans, which have skill building activities. I have looked around, however I can not find a single clan ... can anyone help me out? I just want to learn so anything will do ... thanks in advance!
> [R1]: Learn and fast don't mix. If you want to get good you have to understand how all of it works. I recommend lots of reading and practice on Website A or some other site. I have also never heard of a clan that teaches noobs.
> (Forum D1 Thread #28)

Pertaining to the third theme on order and structure in the web forum site setting, in considering the flexibility of criminal organisations, Ayling (2009) raised an interesting point that the resilience of criminal organisations is dependent on its configuration and the sort of crime it is involved in. In one interview, it was stated that working on a freelance basis on regular projects (as a cybercriminal) was a way to build a relationship with the cybercrime group. Hiring of cybercriminals on an ad hoc basis to contribute to specific goals allows the group to be adaptable.

> I saw a lot of smart script kiddies re-distributing tools that they collected and selling them. There are some people that make the software [crimeware] and those people make big bucks, usually in the thousands ... there were also projects backed by big money, I don't know where the money was coming from, but quite a lot of people were hired for specific projects. There are a lot of the freelancer types that work on one off things ... if these people do a good job, they usually end up working for the same people over and over. I know a lot of packers [individuals specialising in obfuscating malware] that are really good that stay with the same crowd [work with the same group]. (Independent #4)

Paoli (2002) suggested that organised crime groups operating as hierarchies often have set rules to regulate behaviour and maintain order. Likewise, Abadinsky (2007, p. 5) stated that rules are expected in organised crime groups alike legitimate organisations that often have some sort of structure. There were implied references that rules existed on the web forum sites. The [OP] in the follow example alludes to the act of leeching[89] being prohibited.

> [Topic]: Learn how to find admin page for like 90% of websites.
> [OP]: … Leeching is forbidden and may lead to dangerous circumstances …
> (Forum A2 Thread #10)

Also indicating the presence of rules, in the next example the replier [R1] responds to the [OP] suggesting that they have broken the rules of the web forum site. Although not clarified in the discussion, this particular web forum site (Forum E) did not permit discussions related to crimeware, as was outlined in the "rules" section of the web forum site. However, in other discussion threads on this web forum site, crimeware related topics were openly discussed. It would seem rules were not strictly enforced, as crimeware was accessible among various discussion threads.

> [Topic]: I need a FUD keylogger and crypter help me!
> [OP]: I tried many combinations of RAT [remote access trojan] and crypter [crimeware that hides malware from being detected] and re-FUD software [a crypter] … but nothing works … someone can direct me to a keylogger that is FUD ... and subsequent crypter that is compatible? Thanks …
> [R1]: You not read rules here?
> (Forum E10 Thread #19)

Revisiting the idea of *excess* definitions of criminal behaviour by Sutherland (1947), it was suggested that the strength of interactions amongst criminal and non-criminal actors vary with stronger interactions with criminals playing a greater influence on the acquisition of criminal behaviour. Sutherland referred to variables, such as frequency, duration, priority and intensity, which, if increased, would lead to crime. It is conceivable that the ease of

[89] *Leeching*, or a leech, involves the action of benefiting from the efforts of other individuals while not offering anything of value in return.

access to the web forum sites have strengthened such factors; the eight web forum sites were publicly accessible and relatively easy to find through search engines.

Sutherland (1947) specified that the strength of interactions relates to the "the prestige of the source of a criminal or anticriminal pattern" (p. 76). There was indication that discussion threads that were more active were more likely to be exposed to members, thus, its contents would have a greater influence. Discussion threads that have more replies are more likely to be shown on the first page of the discussion thread list.[90] Such discussion threads have a higher intensity, as more individuals may view them and reply to it. It is plausible that such discussion threads have greater significance and exerts a kind of "peer influence" (Akers, 2009, p. 64). The likelihood of members exposed to such discussion threads is greater.

There was indication that certain discussion threads had more replies and views, causing the discussion thread to "bump up" to the first page. The example below shows a discussion thread with a high amount of traffic. Discussion threads that provided an abundance of useful information and were continually updated tended to have more repliers, and subsequently more visitor traffic. Measuring the "intensity" or quantifying the importance of such discussion threads was out of the scope of the study, however an example has been provided for illustrative purposes. Such a case exemplifies a rather unique form of organisation where social groups, the members active in a discussion thread, can be defined based on where most time is spent and consequently where learning is more certain to take place compared to low traffic discussion threads.

> [Topic] Free - Unknown Logger Public V 1.5 - Keylogger - Stealer - Spreader – Worm / Updated
> [OP] Unknown Logger Public V 1.5
> [Picture shown]
> Options:
> 1- Built in Stub [crypter]

[90] On web forum sites, discussion threads that receive a reply are automatically moved to the top of the list. The more frequent replies are posted, the longer the discussion thread will be listed at the top of the list.

2- Get tons of information about the slave, such as Computer User, Computer Name, Computer Total Physical Memory, slave's IP Address, slave's Country, Date, etc. [details of compromised computer]
3- Send logs to SMTP Severs and FTP [transfer details to another server]
4- SMTP (Hotmail, Gmail, AOL, Yahoo) [have details emailed]
[Additional options listed]
Updates for V 1.5:
1- Logs sending bug Fixed
2- Firefox Stealer bug fixed
3- Google Chrome Stealer works for All Versions
4- Assembly Changer added
5- Some small bugs has been also fixed.
[Additional updates listed]
[Download link of tool]
[R1] I vouch this! I can safely say that this group are the best makers of keyloggers out there.
[R2] This looks awesome. I would love to have it. What did u use to program it?
[R3] I would like this, PM me with the link. Thanks.
[R4] This looks really great, would love to have one!
[other replies below]
(Forum A4 Thread #2)

4.7 Conclusion

The observed interactions on the web forum sites bring to light online social interactions suggestive that learning is taking place. The web forum site not only functions as a meeting place but also as a virtual location where its members could converse on topics that relate to crimeware. While the social exchanges were principally text-based interactions, there were also other components to various communication and dealings including the use of visual implements such as screenshots and videos, and in other cases crimeware was made directly accessible in the discussion threads. The web forum sites provided a source to acquire and disseminate knowledge on crimeware and to learn about the techniques of cybercrime. The findings in this chapter also corroborate Holt's (2007) normative orders: technology (individuals certainly need to access a computer and the Internet to visit a web forum site), knowledge (reading, deliberating and participating in discussion threads implies knowledge transfer), commitment (influenced by processes that contribute to learning), and categorisation (manifest as differentiation of members such as novices,

experts, sellers, service providers, members with strong reputations, members with bad reputations, etc.).[91]

As only public interactions could be observed, the interactions observed are certainly not representative of all interactions that may be taking place. The observed interactions only reveal one aspect of cybercrime activities as communication can occur privately. It is also probable that some cybercriminals may not visit such sites.

Interactions revealed activity pertinent to new and infrequent visitors. It was evident that the web forum site members varied in their knowledge, skills and level of competence in the use of crimeware. Certain members provided guidance and direction to members that were new or inexperienced. In certain cases, online tutorials were posted purposely aimed at individuals with little knowledge on hacking and the use of crimeware.

There were many indicators that learning was taking place. Web forum site members posted requests to elicit information and gain access to crimeware. There was also evidence of members "tinkering" with various crimeware tools. If a member had problems with setting up or using a particular crimeware tool, they would post a question to obtain help. Social drivers appeared to encourage certain types of behaviour. For example, when a member made a post of particular value or utility for another member, such behaviour was acknowledged as helpful and, in certain cases, endorsed through vouching.

There were also social dynamics that dissuaded online association. Most members approached unknown or new members with caution revealing a lack of trust. Members would also openly criticise discussion posts that provided little worth. There were also cases of web forum site members targeting other members, primarily through the distribution of crimeware tools that targeted the users of the crimeware tools.

[91] The last of Holt's (2007) normative orders is related to law. The way in which law is perceived among web forum site members is covered in Chapter 6.1.

Chapter 5: The Intersection of Rational Choice and Crimeware

> Crime is a logical extension of the sort of behaviour that is often considered perfectly respectable in legitimate business.
>
> *~Rice*[92]

To recap, the investigation in Chapter 4 focused on the social dynamics occurring within the web forum sites. It was observed that the recurrence of certain behaviours involved online interactions characteristic of learning. The observed discussions affirm certain behaviours are acquired through interaction, as there were social processes that supported, as well as hindered, patterns linked to online learning.

Based on what can be inferred from the content of the discussion posts and the attributes of the crimeware tools disseminated, the aim of this chapter is to examine the motivations of members and their self-interested choices linked to the principle of maximisation. This chapter draws from Cohen and Felson's (1979) routine activity theory as a basis to explain the decision processes of web forum site members. It endeavours to explore the concept of the motivated *rational* offender and relationships between offender choices and observed crimeware tools. To reiterate, the routine activity theory stipulates there are three necessary conditions for a crime to occur: a motivated offender, a suitable target, and the absence of a capable guardian must converge. This chapter investigates the motivation and target aspect of this theory, two requisites for a crime. Although a crucial element of the routine activity theory, the third dimension on the lack of capable guardianship is accepted as a condition and will not be explored in this thesis.[93] Though, it should not be ignored that offender resources are characteristically deployed for the purpose of evading guardians and that all three elements in the routine activity theory impact the design and use of offender

[92] Quoted from *The Business of Crime* by Robert Rice (1974).

[93] A detailed examination of the *lack of a capable guardian* component of the routine activity theory is not provided and outside the scope of this thesis. A narrow view would associate guardians with law enforcement. In its broad interpretation, guardians also comprise of intelligent agents that have played the role of a crime preventer, for example, Internet security products such as sophisticated firewalls and intrusion detection systems. The offender resource relative to the "capability" of the guardian, or how well the guardian detects or stops offender resources, will not be examined. The focus of this investigation is on offender resources that are available to the offender, that is, the emphasis is on the 'motivated offender' and how this may relate to the 'suitable target'. Despite the lack of attention to the 'lack of a capable guardian' part in this thesis, it should not be seen as less important than the other two requisite elements.

resources. Areas that are covered include the technical traits of crimeware itself, the role of criminal innovation, understanding intention based on the design of crimeware, the motivations of different actors involved, the selection of targets or victims which connects to motivation, and lastly introduces the concept of value[94] among the web forum site members.

Motivation precedes the crime. Cornish and Clarke (1987) described motivation as an important factor only at the immediate event before a crime took place, at which time the offender, if already motivated, weighed out the decision on whether to proceed with a crime. Motivation is assumed as a given at the event of a crime. In Wortley's (1998) concept of crime precipitators, it is the events that take place before opportunity that determines motivation. Assuming the motivated offender that is also rational, Tversky and Kahneman (1981) believed that true maximisation was not possible, as an individual would have to weigh all the risks that may not be entirely known (also referred to as bounded rationality); it was posited that offender decisions were based on limited information and dependent on the situation of the offender. Through a survey of 124 respondents disseminated at a computer security hacker conference, Bachmann (2010) identified that individuals desired to engage in actions that *required* a rational thought process. This predilection to *seek* actions in which decisions require a high level of rational thought was also correlated with hacking attempts. That is, the higher skilled hackers hacked more frequently and with greater success; this was also associated with riskier behaviour. The decision-making process of the offender may be dependent on their capabilities and conceivably impacted by the situation and context. A potential offender may make rational decisions during the learning phase, such as when participating in discussions in crimeware communities, but this can differ from the motivation that underlies a decision when

[94] It should be noted that the concept of *value* is seen as subjective. Borrowing from the concept of "bounded rationality", in which offenders behave based on limited information, what is considered of value to the offender can also be bounded. What is of value to an offender may not be of value to non-offenders. Certain offenders may place a higher value on certain items, obtained from the outcome of a crime, over others. To clarify how value differs with respect to causation, Wortley's (1998) "two-stage model" suggests that a crime can be broken down into the crime itself (opportunity) and processes that occur before the crime (precipitators). The concept of value that will be investigated in this thesis is primarily value that is attached to *things* in the events preceding crime (Wortley's precipitators), and is covered in Chapter 5.6, however such *things* of value may also have relevance to value (or simply be the same thing) placed at the immediate event of the crime (opportunity).

engaging in the actual event of a crime. For example, a potential offender who frequents web forum sites to learn how to use a botnet kit, may exhibit elements of maximising behaviour when deciding which botnet crimeware kits are the *most* effective; however, the reason to deploy the botnet, the actual event of the crime can be different, and may not necessarily be related to profit. In light of this, the view of criminals as rational individuals taken in this chapter extends beyond the immediate event of a crime and the narrow stance that monetary profit is the one and only goal. The fact that the offender is motivated is central but there may be more than one motivation, and this should not be assumed to be static.

In criminological research, theories and models are often amalgamated to synthesise new explanations. Cornish (1994) stated that the rational approach could be used as a "heuristic device for structuring criminological debate" (p. 188) suggesting that certain explanations of crime should not be interpreted as dogma. The relevance of criminological theories is through its continuous empirical testing, critiquing for its weaknesses, debating its utility, and exploring its applicability to past and current forms of crime. There has been a widely adopted view that cybercrime is largely driven by financial gain, however, maximising behaviour can be due to non-monetary motivations. For example, profit may not necessarily be the underlying reason an offender aims to maximise their social status among other offenders or when deliberating the most effective technique to target a victim.[95]

With respect to the etiology of crime, the routine activity theory describes crime occurring if the three requirements converge, but fails to take into account the events that precede the crime (relative to the offender) which can be significant in determining the likelihood the crime will take place. The presumption is made that mere convergence is not enough to explain crime, which is an important finding in the study that will be explained further in Chapter 7. For instance, it does not always follow that an individual who actively participates in discussions on web forum sites and has access to crimeware plans to engage in criminal acts.

[95] When discussing theories, I focus on the central tenet. I adopt a more 'loose' interpretation to avoid relegating a theory as a straightforward application to the case of cybercrime. This study aims to advance our knowledge of cybercrime by exploring established explanations of crime, and not only to test its validity.

Ekblom and Tilley (2000) proposed the concept of "resources" available to the offender as an additional requisite of a crime, a seminal concept that is appraised in this thesis and advanced further. Simply stated, a crime is more likely to happen if the offender is "adequately resourced". The question then arises how the offender acquires access to such resources, why certain resources are selected over others and whether rational decisions are indeed involved. Grabosky, Smith and Dempsey (2001) underlined that the more a situation presents itself in which crime could happen, particularly in the case of cybercrime, crime would have an increased probability of occurring. In brief, the Internet simply affords more ways in which crime can transpire, which shifts the focus from offender to targets (the potential victims). The type and nature of cybercrime targets are numerous and varied. A few examples of technology-based targets include websites and servers accessible on the Internet, personal private information and confidential data; if successfully targeted by the offender, it is the institutions, businesses and the general Internet user that are affected. The opportunities for crime are certain to increase with the steady development and growing adoption of new technological devices that interface with the Internet. There is the potential for a crime to happen if the conditions of the routine activity theory are met, however, certain resources available to an offender may also play a factor.

The findings in this chapter indicate there are processes linked to crimeware that correspond with choices made by the offender for the reason to maximise benefit, capitalise on a weakness or to elude discovery from anticipated targets including crime preventers (guardians). The investigation in this chapter will draw primarily from the discussion content on the web forum sites. A small selection of interviews with Internet first responders is included. Real-world instances of crimeware used in the modus operandi of online fraud will be provided as illustrative examples (see Case 2 and 3). Electronic data will also be presented that is specifically linked to data generated from the use of *Zeus*[96] by active cybercriminals (see Case 4 and 5). The analysis in this chapter will refer to general technical features of crimeware tools, but is not intended to be an in depth technical analysis.

[96] *Zeus* was a prevalent crimeware tool at the time the data was collected in 2012.

5.1 Attributes

The aim of this section is to present the important features of crimeware tools. The key traits of crimeware tools that are addressed in this section are its primary or core function, typologies of crimeware, the fundamental ways in which it can be accessed, popularity and prevalence, capabilities with respect to its effectiveness to perform its primary function and the stability of the software, and the relationship between software kits and botnets. Understanding the technical characteristics of crimeware is key to understanding the cybercrime incident, the process of which a crime occurs and the intention of criminals. As uncovered in the discussions observed on the web forum sites, certain software consists of features that suggest such tools were intended specifically for malicious and criminal activities.

Wall (2007) highlighted the role of *viruses* and *worms* as examples of malware with the primary function to propagate or spread. Other forms of software also exists that take the form of programs that perform specific tasks, snippets of code or malicious binaries that aim to compromise the computer of victims. The importance of this section is to present crimeware tools that circulated between 2009 and 2012 on the web forum sites. This section will identify the general characteristics of the various crimeware without delving into its technical operational details. The six main categories of crimeware tools found on the web forum sites have been summarised (see Table 5 below).

Table 5: Key simplified definitions

Key term	Variants and alternate terms	Definition
1. Remote access trojan	Bot kit, botnet kit	Provides backdoor access for cybercriminals
2. Keylogger	Logger, stealer, bot kit, botnet kit, form grabber	Covertly saves and transmits to cybercriminals the keyboard events of victims
3. Crypter	Binder, joiner, packer, obfuscator	Hides malicious files from detection
4. Exploit kit	Attack kit, web attack kit	Performs act of compromising systems and the spreading of malicious files
5. Scanner	Web vulnerability scanner, port scanner, penetration testing tool, SQL injector	Searches for security holes and vulnerabilities
6. Shell	Booter, host booter, DoS tool	Provides command access for cybercriminals to manipulate, destroy, add or download files on a remote system

It is important to note that certain crimeware tools fall under multiple categories such as those listed previously. For example, a remote access trojan, keylogger and crypter can be distributed as a single software package as in the case of *Zeus*. With crimeware becoming increasingly sophisticated with multiple functions available, there is certain ambiguity on the use of terms. Tools such as *Blackshades* is often referred to as "botnet" but is also a tool that provides the functionality of a remote access trojan and keylogger, along with other unique features such as turning on devices like a webcam without the knowledge of the victim, in addition to options that allow the control of a botnet. In a blended attack, certain tools may be used in conjunction to increase the chances of success for the offender. It is not uncommon for *Zeus* to be used along with *Blackhole* (refer to Case 2 and Case 3 in Chapter 5.3). Additionally, certain crimeware may be more effective at performing a particular function compared to other tools designed for a different purpose. For these reasons, categorising crimeware tools can be problematic. Nevertheless, understanding the various features and functions of a crimeware tool is helpful in knowing its intended purpose and a step toward better understanding the motivation of the offender.

The most common tool identified were those labeled as remote access trojans, often referred to as a "RAT" in discussions. Remote access trojans are an example of crimeware that allows, "… some form of remote access and control to the now compromised system

by unauthorised persons" (Kienzle & Elder, 2003). Certain remote access trojans provide features such as monitoring user behaviour through keylogging and access to personal private information on a victim's computer. The following is an example of a discussion thread that reveals features provided in *Blackshades*,[97] a popular remote access trojan at the time of data collection. In the example, the discussion post by the [OP] states the unique advantages of using *Blackshades*, some of which includes its ease of use and visual interface, in addition to technical features such as the capability to compromise computers through instant messaging services. It was evident that certain sophisticated tools such as *Blackshades* provided a comparatively abundant set of features, which is suggestive that considerable time and thought was expended to develop the tool.

> [OP]: Deciding between a RAT, a host booter, or controlling a botnet has never been easier … you get the best of all three - all in one with an easy to use, nice looking interface. You are able to choose between four crisp looking skins, with the default being a very nicely-fitting black theme … does a lot of the work for you - it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ and USB devices …
> (Forum C6 Thread #7)

Within the discussions observed, it was evident there were different remote access trojans distributed. Furthermore, certain remote access trojans had unique characteristics with specific requirements and dependencies to operate them. The following is an example of a remote access trojan offered as an alternative for members that do not have a router. Interestingly, the [OP] is the member responsible for posting *Loki RAT* free for download, but mentions they prefer *DarkComet*, another common remote access trojan.

> [OP]: … About Loki RAT: LokiRAT-Simple and unique PHP RAT. LokiRAT is RAT, which doesn't require Port-Forward [which requires a router], it's using PHP and MySQL on hosting [third party software required to operate the RAT]. It is a very simple and nice alternative to other RATs, especially if you do not have router access or unable to forward ports. This RAT does not need port forwarding. [Features of tool listed] [Download link of tool]

[97] An FBI investigation occurred surrounding the *Blackshades* tool in 2014, a sophisticated RAT, which was distributed and sold in online forums. Over 90 arrests were made in multiple countries in the Blackshades organisation. It was alleged that Blackshades was available for sale at one point for $40 (US DOJ, 2014).

[R1]: Nice share.
[R2-OP]: You're very welcome … I personally prefer DarkComet, but I have purchased a VPN [a proxy service] to get it to work properly.
(Forum H4 Thread #19)

Crimeware tools had unique names or *brand* labels (see Appendix 1 for a full list of the crimeware tools identified in the study). Within each grouping of crimeware tool from the six types identified, there were multiple options of tools that circulated on the web forum sites. The following example shows a discussion thread that contains 28 different keyloggers available for download.

[OP]: Keyloggers / 1. Albertino Simple Keylogger / 2. Ardamax 2.8 Keylogger / 3. A++ Keylogger / 4. Basic Keylogger / 5. BKB Keylogger / 6. Black Oil v1.1 … [20+ other keyloggers listed] … / 27. Silent Keylogger v1.6 / 28. Vaqxination v5.1 [Download link of tools]
(Forum G3 Thread #2)

There was also evidence that certain crimeware tools were more popular. In the following example the [OP] makes a reference to *Citadel* being used widely.

[OP]: A glimpse inside Citadel: [Screenshot of the tool] Looks pretty damn hardcore …
[R2]: Citadel Zeus is used the most this year, and yeah, pretty hardcore as you said.
(Forum F4 Thread #7)

Certain crimeware tools were clearly more prevalent, and easier to access for this reason, than other tools that were disseminated. [R5] in the following example makes a comment that discussion threads related to *DarkComet* has been relatively common.

[OP]: … I'm making this guide because a lot of people are having problems with it. In this guide I will explain how to: 1. Set up no-IP [a required component for DarkComet to work]. / 2. Portforwarding [a step required before configuring the tool]. / 3. Set up DarkComet. / 4. Create a silent java drive by [a technique used to compromise computers of unsuspecting victims that visit a website] …
[R5]: I've been on this forum for just over 4 hours and I already can see this "DarkComet" taking it over. I'm sure there is a tutorial section here, post there not in this section. I would like to see some decent threads soon.

(Forum A1 Thread #17)

The next case is of a thread in which the "best" keylogger is discussed. The three members in the thread recommend different keyloggers, namely *Sckeylog*, *Emissary* and *iStealer 6*. There was indication that the web forum site members had different favoured choices on which keyloggers were the most useful or effective. It was evident that different crimeware tools had distinguishable attributes that had an influence on personal preference.

[Topic]: … Darkcomet 5.3.1 … Detailed guide.
[OP]: What's the best keylogger? I heard Sckeylog was pretty good.
[R1]: I recommend Emissary keylogger available from the forums.
[R2]: IStealer 6 is the best in my opinion. Uploads to website, which is good feature, also can be downloaded from [Website name redacted] …
(Forum E10 Thread #4)

Certain crimeware tools were freely available for download while others required a cost. In the following example, [R4] makes a distinction between "public" and "private" RATs, which refer to tools that are freely downloadable and those requiring a fee, respectively.

[Topic]: Cybergate v1.07.5
[OP]: [Features of tool listed] [Download link of tool] …
[R4]: This is the best public free RAT. The best private RAT in my good honest opinion is Blackshades. It offers many things like stability and functionality …
(Forum E8 Thread #14)

Sood and Enbody (2013) used the term "Crime-as-a-service" (CaaS) to refer to aspects of the underground crimeware market that mirrored legitimate businesses. On the web forum sites, crimeware tools could be accessed through a rental or leasing model for temporary use or provided access through an intermediary party. The following is an example of one member soliciting a botnet rental service. [R1] states they are willing to offer help for a fee with up to 20,000 bots available under their control for use. Such cases reveal that indirect access to crimeware is possible.

[OP]: Does anyone in here have a botnet running where the clients have dynamic IPs and can be used as socks proxies to make http and https calls? I'm not interested in

> becoming the owner of such a botnet … The clients should use a fast Internet connection and be available 24h per day in the best case. Let me know how much IPs you can offer and how much you like to get per IP (per 24h or www call).
> [R1] Yup - USA only. No proxies will be up 24/7, but there are multiple IPs per city. 20,000 made available at all times. $2500/month – BTC [bitcoin] only.
> (Forum D3 Thread #36)

Effectiveness in performing a specific function and stability influenced the demand of certain crimeware tools. In the following example, the [OP] states that they had trouble using *Umbra*.[98] The repliers [R6] and [R8] make a reference to the stability of the tools. In this particular case, it should be noted that stability refers to the dependability of crimeware to accomplish a task. The discussions support that reliable tools, that worked and were less prone to have problems, were in greater demand than less reliable tools.

> [OP]: So I am looking for a good free or cracked [circumvented software] loader. It doesn't need to be a form grabber [keylogging function] or DDoS [ability to perform denial of service attacks] or anything. Just reliable on holding bots [the ability to maintain and manage a botnet] and executing download updates [uploading updated fixes and improvements of the malware to the compromised computer]. No Cythosia, please. Umbra never wants to work with my host … So please post recommendations!
> [R6]: Yeah SpyEye … it works, and its stable …
> [R8]: Use Umbra loader and Andromeda cracked. Umbra loader is a free delphi HTTP bot that works good and stable. Works good for bot holding [maintain a botnet]. Andromeda is the best one I have used and its really hard to kill that bot, and its really stable.
> (Forum F4 Thread #12)

Another attribute of crimeware is whether it has been *cracked*. Such tools have been modified to circumvent restrictions that originally only allowed certain prescribed users to use them. The following is an example of a replier [R2] who refers to a cracked version of a

[98] A *loader* functions similarly to a remote access trojan with the more narrow function that involves uploading a malicious "payload" to a compromised computers or the botnet. The function of a loader is to "off load" malware onto a victim's computer.

popular crimeware tool used to target banks known as *Carberp*.[99] [R2] replies that the cracked version of *Carberp* does not work and is unusable.

> [Topic]: Best Banking Bot?
> [OP]: Hi guys, how are you today? Hope to be fine. I want to know what is the best banking bot
> Zeus, Zeus Ice, Zeus Citadel, Spyeye ... or what? And what is the best version of Zeus? Thanks a lot.
> [R2]: Latest version of Carberp, the cracked versions are garbage.
> (Forum F4 Thread #10)

There were also examples of *backdoored* crimeware tools in which members were targeting other web forum site members. It was evident deceptive practices were directed between members, as raised in Chapter 4.5. In the following example, the [OP] makes an inquiry about which remote access trojan is the best for use. [R1] makes a reference to *SpyNet* being potentially backdoored implying that it is not safe to use.

> [OP]: I don't know which RAT is the "best" so if you guys can recommend me your best RATs, it would be great.
> [R1]: Easiest to use would be DarkComet and CyberGate. Hell, I'd even put SpyNet in the list, but I remember the rumor of it being backdoored. Blackshades is also a great one.
> (Forum G3 Thread #22)

Ollman (2009) suggested that the actors that control botnets should not be assumed to be the same actors that employ crimeware tools or who create botnets. Likewise, the actors that create crimeware tools may be different from those that distribute and use crimeware tools. There is a lack of criminological research about botnet controllers and the crimeware they use, however certain crimeware tools identified on the web forum sites can be linked to widely prevalent botnets. Case 1 below reveals the 64 largest botnet types that were found among Internet IP addresses in Australia in 2012. The botnet groups can be linked to specific crimeware tools, for example, *Carberp* and *Zeus* are identified as prevalent botnets,

[99] *Carberp* has similar functionality to *Zeus*, *Spyeye* and *Citadel*. Such crimeware tools have also been referred to as 'banking trojans', as they include features aimed at targeting financial institutions (Donohue, 2013).

as found in the list, and the crimeware to create such botnets were also circulated on the web forum sites, as revealed in previous examples.

Case 1: Top 64 identified botnet types between January 2012 and December 2012[100]

Artro	Darkmailer	Generic	Nachi	Silon
Asprox	Delf.FZ	Gheg	Netsky	Sinit
Avalanche	Delf.HPT	Goldun	Oddbob	Slammer
Beagle/Bagel	Dirtjumper	Gozi	Ozdok	Spyeye
Blaster	Dlena	Grum	Phatbot	Stormworm
Bobax	DNSChanger	Hellogirl	Ponmocup	Toxbot
Carberp	Donbot	Iflar	Poof	Virus1
Cimbot	Downadup	Kelihos	Pushdo	Virut
Clampi	Feodo	Lethic	Ramnit	Zapchast
Conficker	Festi	Maazben	Reposin	Zeus
Cp	Fivetoone	Machbot	Russkill	
Cutwail	Flashback	Mebroot	Rustock	
Cutwail2	Gbot	Mydoom	Sality	

Note: Refer to Chapter 3.6 (Table 4) for further details on the source of the data.

5.2 Innovation

Innovation is often associated with the improvement of *legitimate* technology. However, criminal innovation was also evident among the web forum site activities, which to some extent is reminiscent of tinkering. Discussions in the web forum sites pointed toward activities to fix and improve crimeware incrementally. In other cases, certain web forum site members attempted to install and operate crimeware. Three themes arose pertaining to innovation, namely the basic case of innovation through the development of new crimeware tools, software versioning that reflects advancement, and the open source effect of certain crimeware source code that are freely accessible.

[100] As highlighted by Ollman (2009), each of the 64 "families" of botnets identified can consist of multiple botnets. For example, let's say a single botnet "family" such as *Zeus* consists of 100 different botnets. The 100 different *Zeus* botnets may be controlled by multiple parties, and each party may consist of multiple individuals. The botnet "family"-to-cybercriminal relationship should not be assumed as one-to-one. The number of actors involved that control botnets is unknown. However, botnet activity that are attributed to a particular "family" can be estimated, which have been identified by botnet monitoring agencies and Internet security companies. Generating an accurate estimate is difficult, as it is also expected that there are botnets *in the wild* that have yet to be discovered.

Cornish and Clarke (1987) suggested that the rational choice view of criminals could be extended to include the idea of "choice-structuring properties". Their idea presumes that the choices available to an offender depend on the type of crime. Effectively, it is the crime that affects the decision and pathway of the offender that decides to engage in a crime (Felson & Clarke, 1998). It is conceivable crimeware can also play an influential role in the choices made. In a study between drug traffickers and terrorist groups, Kenney (2007) described the idea of "competitive adaptation" and that criminals who succeed may be due to the simple fact of going unnoticed by law enforcement. The ability to evade detection from cybercrime responders and countermeasures may help to prolong the success of criminals in the acts of crime. Purposefully adapting one's behaviour may also assist in avoiding detection. In describing the displacement of crime, Reppetto (1976) noted that criminals repeatedly engage in the same crime but alter the way in which it is carried out.[101] In the case of cybercrime, such examples are exemplified through the different crimeware tools available on web forum sites; access to different tools by offenders allows for cybercrime to be carried out in diverse ways.

Ekblom and Tilley (2000) remarked that the changes in offender behaviour was a gradual progression in which offenders would change their modus operandi to evade the crime prevention measures designed to stop them. It was stated that crime prevention entails change and innovation, which is anticipated and in turn neutralised by the offender, occurring as a cycle. The research indicates that certain offenders were choosing to innovate through the development of crimeware, not only to circumvent detection, but also to improve the crimeware tools for the benefit of web forum site members and the users of crimeware tools. Innovation may also occur for the purposes of outperforming other similar crimeware tools in the same category or with comparable features.

Cybercriminals have shown their innovativeness since the first incidents of cybercrime on the Internet. However, it was around mid 2000 that a transformative change occurred with

[101] Reppetto (1976, p. 168) categorised displacement as temporal displacement (commission of a crime at a different time), tactical displacement (changing the way in which to target the same victim), target displacement (selecting different targets), territorial displacement (targeting based on familiarity or whether the target is in close in proximity to the offender) and functional displacement (offenders engaging in different types of crimes).

the introduction of crimeware kits (Symantec, 2010). An observation was made in an interview with one Internet security professional that has been working in the computer security field for over 15 years that cybercrime offences have evolved.

> We first started seeing crimeware kits in 2005-2006 and it has changed drastically over the years. They are now [in 2012] much more complex. This is understandable because when technology changes, the techniques for crime need to change too. (Private sector #1)

This evolution of cybercrime was also noted in another interview who highlighted an increase in financially focused cybercrime activities happening around the same time period along with the growing prevalence of botnets.

> I did notice certain changes over the years since my former blackhat days. In the 90s it was more about seeing what was possible, not many people were in it for money. After mid 2000 is when the credit card fraud scene started getting big. Now [since mid 2000] it's all about the data … There are those big intrusions where websites are hacked and peoples details that are taken … botnets became popular about the same time. Botnets are similar except way more computers are involved. Death by a million cuts is the way I see it. That's where the problem is [referring to botnets], not the big hacks. (Independent #4)

Choo (2007) predicted that new cryptographic designs of malware would develop over time. In two of the interviews, it was stated that cybercriminals were indeed employing the use of more advanced cryptographic techniques from earlier releases of crimeware tools. According to Bachmann's (2010) survey of hacking conference attendees, the use of more advanced malware suggest offenders are engaging in behaviour connected to higher risk, if malware sophistication is associated with skill.

> In the case of Zeus, the early versions did very little to hide its tracks using basic almost non-existent encryption techniques. Later versions of Zeus used more complex techniques using RC4 keys [an encryption technique], which is actually not that advanced, but definitely an improvement making it harder to investigate. (Independent #5)

> Hiding your tracks is a big thing. The good ones [cybercriminals] I know hide their track using the latest encryption technologies when they communicate with botnets.

> You heard of fast fluxing? It's just one of many techniques to hide your botnet control servers. The government is starting to monitor the Internet much more closely ... it's getting more riskier, so they have to be extra careful now. (Independent #4)

There was indication of the active development of crimeware tools on the web forum sites. The following two examples reveal the [OP] in the midst of developing crimeware tools. A reference is made to the tool being in the "beta" stage, which indicates that the software is currently under development and testing, and not yet ready for distribution.

> [Topic]: Development - Beta Bot - Coded in C++ -- Updated: 2/12/2012 / Beta testing started
> [OP]: … Notice: Beta testing in progress - Round #4 of tests. Release date is still postponed until testing is finished. Testing is private only - Please do not ask for test builds …
> [List of tool features]
> (Forum A9 Thread #1)

> [OP]: This is the 'beta' release of the new Cerberus RAT. I'm sure you've heard of it. It's great.
> [Screenshots of tool] [Download link of tools]
> (Forum E8 Thread #5)

There were also discussion threads that guided users on how to create their own keyloggers. In the following example, the high-level steps to create a keylogger are posted. Such discussion threads conceivably promote the development of new crimeware.

> [Topic]: Making your own Keylogger
> [OP]: ... Basic Concepts: What needs to be achieved. Ok, now lets plan our program, what should such a keylogger do and what it should not. Significant difference to previous section [referring to another discussion thread] is in the sense that here we shall discuss the logic, the instructions that our program will follow. Keylogger will:
> 1 – listen to all the keystrokes of the user.
> 2 – save these keys in a log file.
> 3 – during logging, does not reveal its presence to the user.
> 4 – keeps doing its work as long as the user is logged in regardless of users actions ...
> (Forum B1 Thread #33)

Another signal of criminal innovation is software versioning. Software versioning is a system in which software is designated a number to signify major or minor changes that have been made. The following example indicates software versioning in use when a reference is made to *Zeus 2.1* and *SpyEye 1.3.45*. Note that an incrementing of numbers after the first decimal place denotes a minor change. Software versioning is a standard process used in the legitimate software industry to label and delineate revisions of new software. It appeared such typical practices used in general software development are mimicked in the process of developing crimeware. Most, if not all, crimeware tools identified in the web forum sites use software versioning, an indication that tools were undergoing constant improvements.[102]

> [Topic]: Need botnet like Zeus
> [OP]: Hello friends. I am new here and also new to botnet world. I used cracked version of Zeus 2.1 and Spyeye 1.3.45 but in both I am having issue … Can someone tell me how to fix it or tell me some botnet, which is like Zeus and works with all browsers?
> (Forum F4 Thread #6)

Discussion threads indicate open source[103] development practices taking place, better described as the sharing of source code.[104] The source code of crimeware tools openly available presumably allows any web forum site member the opportunity to make changes to add or improve upon its features. The sharing of source code also provides the opportunity for members to learn how the underlying technical aspects of crimeware perform its function. In the following example the [OP] specifically seeks open source botnet code for the intention of using it to create a botnet of 5,000 to 10,000 compromised computers.

> [Topic]: A good open source HTTP Botnet?
> [OP]: Hello! Do you know a stable - 5000 to 10000 user - open source HTTP Botnet?

[102] In Appendix 1, there are over 300 crimeware tool *brands* listed that have been identified in the web forum sites – the version numbers were not provided in the list.
[103] *Open source* is a model and philosophy for software development that allows for the underlying code of a software program to be updated by anyone.
[104] *Source code* is a collection of programmed instructions written by humans that are the building blocks of a software program.

> I know bot coded in VB6 [programming language] but I don't know if it is stable. Also I know Umbra Loader V1.1.0 but I don't know if it very stable. And I know VertexNetLoader with an open source server but I don't know if it stable because it is not the official server source [from the original trusted source]. And now I search for an open source botnet, not a leaked cracked version. Thanks in advance.
> [R1]: Try Zemra … or small loader 2008 source …
> (Forum F4 Thread #2)

An interesting implication of the adoption of open source approaches is that it allows web forum site members to enhance and customise, with little effort, pre-existing crimeware. It was suggested by one of the interviewees who came from an online fraud mitigation role at a bank that it was the sharing of source code that was a chief concern for fraud that targeted banks.

> Leaked source code [of crimeware] is the main cause of the problems because people make variants which are in most cases are made better than it was before … and then they release it. The hackers are in a way working together if you think about it that way. (Public sector #2)

Article 1: Zeus + Carberp = Zberp

In 2014, a variant of crimeware known as Zberp was identified which allegedly consisted of an amalgamation of source code from both Zeus and Carberp, two different crimeware tools designed to steal from banks. The Zeus source code has been known to be circulating on forums since 2011. The source code for Carberp was rumoured to have leaked on forums sometime in 2014. The hybrid tool was stated to be better at evading detection from security products.

Article 1. *Criminals fuse Zeus, Carberp code for more sinister trojan*. Retrieved from http://www.scmagazine.com/criminals-fuse-zeus-carberp-code-for-more-sinister-trojan/article/348880/ (Walker, 2014)

5.3 Intention

A fundamental component of criminal law is determining whether a criminal has a *guilty mind*[105] when committing a crime. Cornish and Clarke (2003) referred to the intention of a criminal as *readiness*, which is influenced by some underlying motivation. In criminal law,

[105] *Guilty mind* refers to *mens rea* in latin, while *actus reus* refers to the physical component. These two elements are required to determine criminal accountability.

intent and motive are distinct, referred to as intention and motivation respectively in this research. The definitional distinctions are not important, however, intention concerns the immediacy or the state at the moment, while motivation centres on more deep-seated dispositions or a rooted purpose. In certain parlance, such terms may be used interchangeably or have the same meaning. The aim of this section is to *infer intention* based on the designed features of crimeware tools.[106] There were three main themes that arose: tools that are deliberately designed for cybercrime, tools unintentionally used for cybercrime that have criminogenic features, general attack vectors[107] or techniques used to engage in cybercrime that are a signal of intention, and lastly, the decision to use multiple tools in combination.

The first theme identified is based on the deliberate design of tools for criminal purposes. Certain crimeware tools were designed to *spread* malware such as the case of spam containing malicious website links[108] that aim to infect victims (Alazab and Broadhurst., 2014). Likewise, exploit kits are intended to spread malware infections with the aim to infect computers that visit a compromised website. Other tools such as crypters are intended for use to *evade* detection from security detection products. In such situations, the cybercrime techniques used are an outcome of crimeware, and in other cases multiple crimeware may be used in conjunction to commit a cybercrime that is multifaceted. It should be noted that such actions are a consequence of the use of crimeware and signals the intention of a malicious or criminal act. The crux of the point raised in this section is that the design of crimeware tools does not necessarily dictate if it will be used for cybercrime, as an individual may download a crimeware tool for non-malicious use, however it is clear that certain tools have no other function but for the purposes of cybercrime.

---

[106] The point is to draw conclusions on the purpose of a particular crimeware or an action relevant to crimeware. Crimeware in itself cannot (literally) show intent, as it is certainly not an autonomous entity, however certain crimeware may have general properties that delineate it from other forms of software.

[107] A *general attack vector* is a term used in the Internet security field that refers to common methods cybercriminals use to target victims. Examples include emails with file attachments (if opened) that aim to infect a victim's computer and malicious websites (if visited) that seek to propagate malware (Alazab & Broadhurst, 2014).

[108] In the study, emails sent to potential victims included malicious web links. The email would also contain content that would trick a potential victim into clicking the web link. Once such a web link was clicked, the victim's computer would be compromised. Refer to Case 2 and 3 for examples.

On the second theme, it was evident that certain crimeware tools disseminated on the web forum sites were deliberately designed to engage in cybercrime activity while other tools were unintentionally, from the perspective of the party that created it, being used for cybercrime. Ekblom (2014) suggested that structures in the physical environment could be "designed out"[109] to decrease the likelihood of crime. However, in the case of certain tools originally intended for legitimate use, the same designed features for legitimate use can also be used for illegitimate purposes. Designing out such features would not be feasible in such a case.[110]

There was indication of software, originally intended for legitimate use, may be used for illicit aims. The following three examples show tools originally meant for legitimate use, namely *Acunetix*,[111] *Havij*,[112] and *Metasploit*,[113] being distributed on the same web forum sites where crimeware tools deliberately designed for criminal purposes are found. The three tools are available in the Internet security market as products to be used for the purposes of protecting systems.

> [Topic]: Acunetix Version 8 Web Vulnerability Scanner
> [OP]: Audit your website security with Acunetix Web Vulnerability Scanner. As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information and customer lists. Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases. [Download like of tool] [Contact details of the OP]
> (Forum H4 Thread #2)

> [Topic]: Havij v1.16 Pro Portable Cracked
> [OP]: Here is a cracked version. Registered / Full Working [Download link of tool] Have fun.

[109] Essentially removing features that make crime easier to carry out.
[110] The ramifications for crime prevention, specifically responses to crime through criminalisation and its unintentional effects on the legitimate use of crimeware are covered in Chapter 6.5.
[111] *Acunetix* company website: https://www.acunetix.com
[112] *Havij* is a product developed by an Iranian security company known as *ITSecTeam*. Details can be found here: http://itsecteam.com (the website shutdown in late-2015 but an archived snapshot of their website can be found at https://archive.org/web/)
[113] *Metasploit* is marketed as a penetration test tool by the company *Rapid7*. Their company website is: http://www.rapid7.com

[R1] Anyone have Havij 1.17?
[R2-OP] I didn't know there was a 1.17 version yet. The 1.16 with multi threading is the newest.
[R3] 1.17 version is good ...
(Forum C5 Thread#3)

[OP]: Tutorial - Hack Windows XP with Metasploit – high quality pictures
[Screenshots provided with directions]
(Forum A5 Thread #10)

There was indication that such tools were used for malicious purposes. The following example is a discussion thread that provides a description on how to illicitly hack online email accounts using *Metasploit*, a tool developed by a legitimate company that purports to prevent such cybercrime activities.

[Topic]: Extract [hack into and steal] emails from any website
[OP]: Salam, today I'll show you how to get emails from any web you want [hack online email accounts]. The thing I'll be using is Metasploit ... Extracting emails using Metasploit so get your hand buzzy … [Explains how to use the tool]
(Forum C4 Thread #18)

It emerges that certain Internet security companies that create such software have customers that have both legitimate and illegitimate intentions. Cybercriminals use such tools to attack hack into websites, and at the same time, organisations behind the website conceivably hire legitimate professionals to protect their website who use the same tools. Such tools could be considered "dual-use" as they serve both criminal and non-criminal purposes (Sommer, 2006). Whether these tools should fall under the "crimeware" umbrella is controversial which presages that all such tools would be considered illegitimate.

The third theme relates to the techniques of cybercrime that are extension of the design of crimeware. There were four recurring cybercrime techniques that were discussed in threads, namely the spreading of malware, creation of botnets and evading detection, and blended attacks. Choo (2007) noted that botnets are used to amplify the spreading of files that aim to infect computers and create further botnets. In other words, botnets can be used to spread

malicious files, and the spreading of such files subsequently creates further bots. Wall (2007) also observed this cyclical pattern between malware and botnets (p. 152).

The first recurring cybercrime technique is the intention to *spread* malware through crimeware tools. The [OP] in the following example makes an inquiry related to steps required to infect multiple computers at their school using a remote access trojan called *Turkojan 4*. The act of spreading a remote access trojan would subsequently allow the offender to both control a victim's computer and steal data from it.

> [Topic]: How to spread my RAT
> [OP]: Hello ... I want to know how to spread my RAT. I'm using Turkojan 4, and I want to spread on my school system, so that I can just extract it from my USB to the computer. But I want all computers to be infected. Thanks guys. I'm already studying about keyloggers and stuff. Thanks.
> (Forum D1 Thread #9)

The second recurring cybercrime technique is the *creation or control of a botnet*. In the following example the [OP] mentions being knowledgeable of a spreading technique that can infect 10,000 computers per week. Notably, the [OP] states that s/he does not wish to reveal their strategy without a fee, indicating that their knowledge (cybercrime technique) has a certain value associated with it.

> [Topic]: Spread your server very efficiently 10k+ downloads/week
> [OP]: Hi guys! It's a very, very powerful method, so actually I hope you can understand. I don't want to tell it for nothing [give out the information without receiving something in return]. If you have a FUD [fully undetectable] server, you can make about 10k bot in a week. Send me a private message, or add me on Skype: [username redacted], and we can make a deal. Good luck!
> (Forum B1 Thread #15)

The third recurring cybercrime techniques involve *avoiding being discovered*. The [OP] in the previous example mentions the requirement of having a "FUD", or fully undetectable, server when building a botnet. Evading detection from security products is also a signal of a malicious action and a common theme found in the web forum sites. Tools that aim to provide the capability to conceal its activities from victims were crypters. In the next

example, the [OP] posts a crypter available for download. [R3] and [R5] state that the crypter is no longer working as their files were detected.

> [Topic]: Crypt0n0m1c0n v1 FUD 100% - 01/04/2011
> [OP]: [Tool posted for download]
> [R3]: Unfortunately it has already seen by a lot of antivirus engines.
> [R5]: Oh nice post but unfortunately, now it's being detected. Please re-FUD.
> (Forum E8 Thread #11)

The fourth theme relates to the use a combination of different tools for a particular goal. Crimeware tools could be used in conjunction with each other, which conceivably enables, and improves the realisation, the eventual cybercrime being carried out by the offender. The following example shows a member seeking a crypter to use along with *Zeus*, which would decrease the chances of *Zeus* being discovered by a victim.

> [Topic]: I need a crypter
> [OP]: Please any verified seller here. I am serious and ready to deal. I need a strong crypter for Zeus. Any persons that has it should PM me here. Thanks.
> (Forum C9 Thread #13)

The point of interest in the next example is the response by [R7] who mentions that they used both a loader, a specific form of a remote access trojan, and *IPKiller*, a tool designed for the purpose of engaging in DDoS attacks over the Internet. It is certainly conceivable that cybercrime may be dependent on the availability of precise tools, without which a cybercrime event would be improbable. For example, without having access to the loader or *IPKiller*, it is probable that the web forum site member would not be able to carry out the act.

> [OP] I was just wondering before I buy it if there was any better software than IPKiller because I would like to use it to build up a powerful botnet, but didn't want to get it and find out it is not the best. Thanks for reading and I hope you can help
> [R7] That's true. I mostly herd my bots on a Loader and then port[114] them to IPKiller -

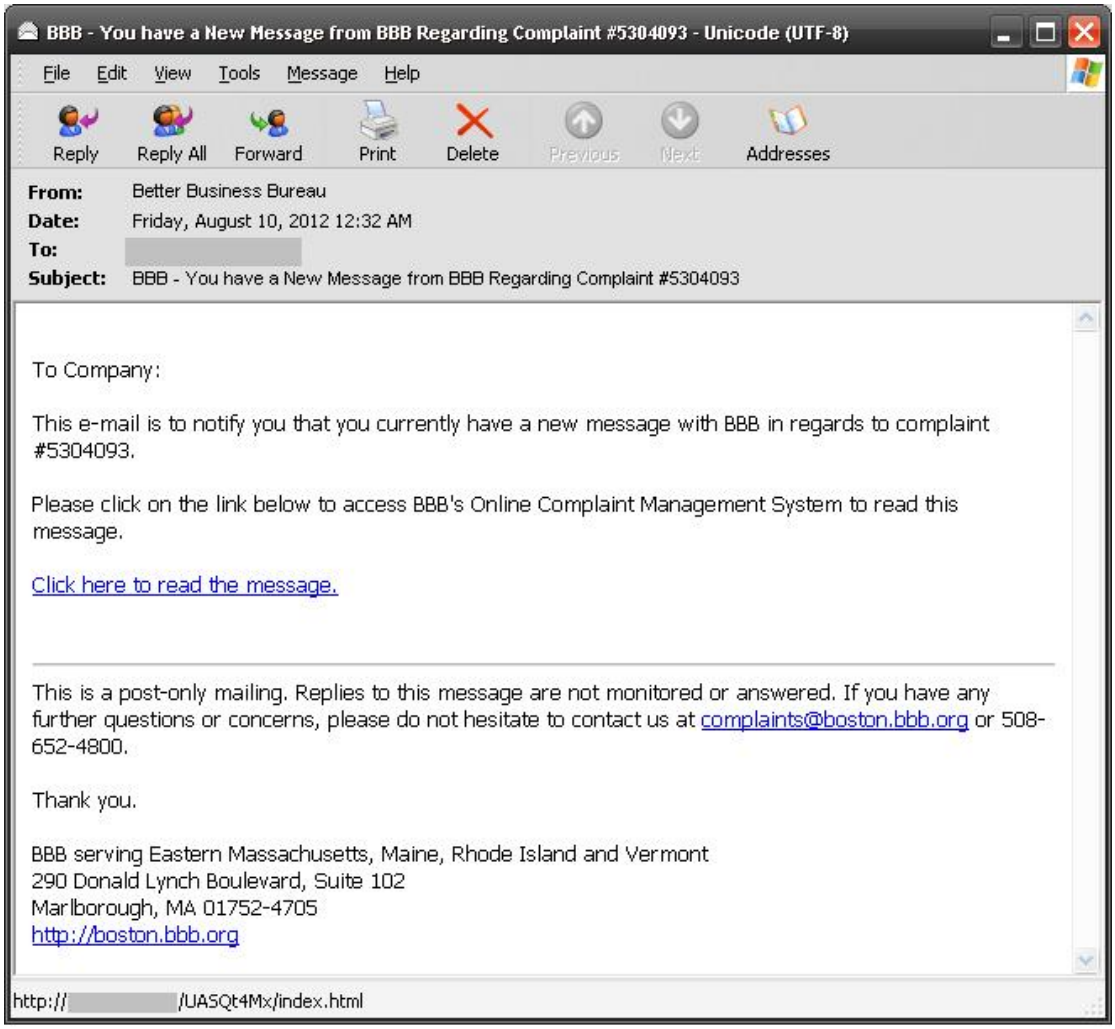
[114] *Port*, or porting, in situations used with botnets involves transferring control of one botnet kit to another. For example, a cybercriminal may use *Zeus* crimeware to control computer X and can "port" the botnet to use *Carberp*, a different crimeware to subsequently take control of computer X.

about 200. IPKiller can hold as much bots as your Internet connection can. (Forum A9 Thread #14)

For illustrative purposes, Case 2 and 3 are presented to reveal real-world cases of a common cybercrime technique used by cybercriminals. It exposes the crime commission process that occurs online that involve the use of email spam, an exploit kit and botnet kit. It also provides insight into how spreading occurs (over email), the act of compromising of the target computer (exploit kit), and the eventual control of the target computer (creation of a bot or botnet). Although deceptive practices such as social engineering directed towards general Internet users was not observable in the web forum site interactions, the examples reveal such techniques of cybercrime. For Case 2, an email was received by a victim, which was allegedly sent from the Better Business Bureau. For Case 3, an email contains details on a PayPal transaction that was allegedly made. In both examples, the cybercriminal uses social engineering techniques to deceive a potential victim into clicking the website link contained in the email.

Case 2: Better business bureau fraud

The below example demonstrates a real case of a technique used by cybercriminals, where a spam email is used along with an exploit kit and a botnet kit. Certain technical details have been masked in the explanation. An email is sent to a potential victim by a cybercriminal under the guise of a legitimate email from the "Better Business Bureau". The email appears official which also contains contact details such as an email address, phone number and physical address. The potential victim is directed to click on "Click here to read the message".



After the victim clicks on the link, they are directed to a malicious website hxxp://accessoltenia.ro without their knowledge. From this website, they are further redirected, unbeknownst to the victim, to a series of other malicious websites as shown below. Of particular interest is one of the website paths containing "tid6mian" which is a specific folder name used in the Blackhole exploit kit. After further redirections, and without the knowledge of the victim, the malicious file 24XiWo1.exe is secretly uploaded to the victim's computer via the Blackhole exploit kit. It is the Blackhole exploit kit that is working in the background, hidden from the user, that is able to upload the file, usually by taking advantage of a security hole on the victim's computer.

hxxp://accesoltenia.ro/wTJp5vGm/index.html
hxxp://www.ceranelli.it/ioDD7kcz/js.js
hxxp://66.55.89.149:8080/tid6mian.php?q=c71c74d4ef655656
hxxp://66.55.89.149:8080/Oper.jar
hxxp://www.giglio.es/24XiWo1.exe

The suspicious file 24XiWo1.exe is associated with a signature a5117d4818219a6e2f0d48471d3a0ae0599d703d, known as a hash or unique "footprint" of the file.

Upon checking this signature on VirusTotal.com, a free online service that identifies malicious files, the file is identified to be malware associated with *Zeus*, a prevalent botnet kit.

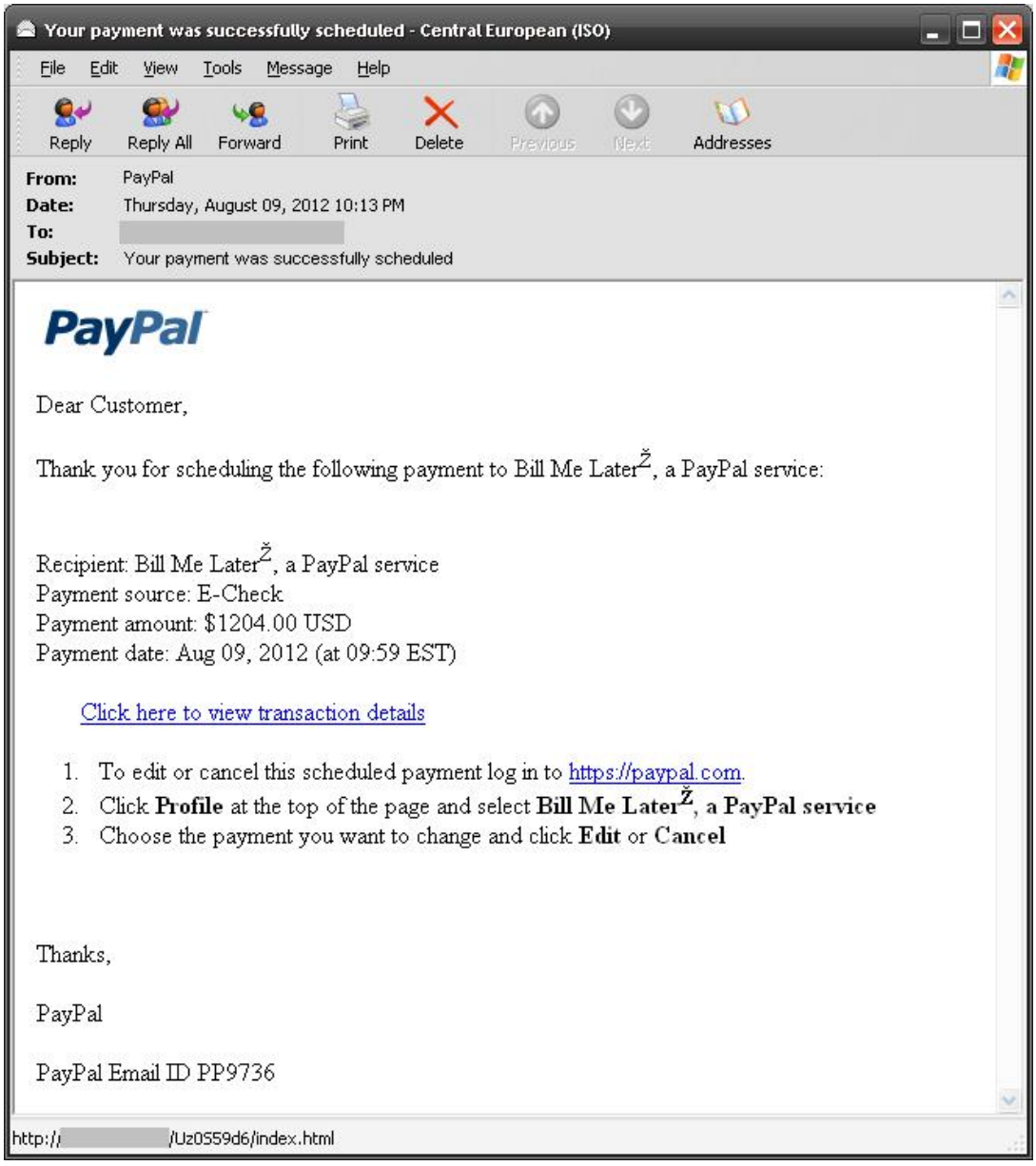
File name: 24XiWo1.exe
File signature: a5117d4818219a6e2f0d48471d3a0ae0599d703d
File identified as: TSPY_ZBOT.SM39 (Zeus)

After *Zeus* is covertly deployed, the cybercriminal has access to the contents of the victim's computer. The cybercriminal has the potential capability to monitor when the victim visits an online banking site or accesses other sites such as email through their web browser. Internet security reports refer to such events as a man-in-the-middle attack, as the cybercriminal is able to relay web browser interactions of the victim to their location.

Note: Refer to Chapter 3.6 (Table 4) for further details on the source of the data.

Case 3: PayPal fraud

The next case is similar, where an exploit kit is used along with botnet kit. An email is sent to a potential victim under the guise of an official email from PayPal. The email appears to be legitimate purporting to be sent from PayPal, as shown below. Interestingly, the email shows that a transaction of $1,204 USD was made. As the victim is unlikely to have made such a transaction, they are lured into clicking the "Click here to view transaction details".



After the victim has clicked on the link, they are directed to a malicious website hxxp://hotelionion.com without their knowledge. As mentioned in Case 2, the website path "tid6mian" is associated with the Blackhole exploit kit. After the victim is surreptitiously redirected through a series of additional malicious websites, the file xWP.exe is secretly uploaded to the victim's computer.

hxxp://hotelionion.com/81shTho6/index.html
hxxp://adanaegemengazetesi.com/6xwEVkGt/js.js
hxxp://50.116.59.71/tid6mian.php?q=w5sa5su1wthouoz6
hxxp://50.116.59.71/Oper.jar
hxxp://etradi.webgenshop.nl/xWP.exe

The suspicious file xWP.exe is associated with a signature ac8051e4adaeaad0a5554c2042e970baaa092a7b, which is the "fingerprint" of the file. Upon checking

this signature on VirusTotal.com, the file is identified to be malware associated with the botnet kit known as *Zeus*, similar to Case 2.

File name: xWP.exe
File signature: ac8051e4adaeaad0a5554c2042e970baaa092a7b
File identified as: PWS-Zbot.gen.aft (Zeus)

Alike Case 2, after *Zeus* is covertly deployed, the cybercriminal can monitor and capture data when a victim goes to sites they typically visit daily (email, online shopping, banking) through their web browser.

Note: Refer to Chapter 3.6 (Table 4) for further details on the source of the data.

5.4 Motivation

The intention to commit crime may be numerous for the criminal, while motivation describes its broader driving force. Referring to the routine activity theory, Cohen and Felson (1979) stated that whether a crime took place was largely dependent on the circumstances of suitable targets, with the offender assumed to be *already* motivated, or have the *intention* to commit crime as emphasised in the previous section, immediately preceding the event of a crime. A narrow interpretation of the routine activity theory would suggest that the offender is assumed to be deterministic to some degree; either the offender has an impelling purpose or lacks a reason to commit a crime. As revealed in Chapter 4, motivation may be acquired through socialisation with other actors online. In the cybercrime scenario, the motivation of an offender may be a necessary condition for a crime to transpire that is "learned" through past interactions with active offenders. However, motivation alone may be insufficient to realise the opportunity of crime without access to certain offender resources such as crimeware.[115]

Specifically for cases of online fraud, Hutchings' (2013) research described motivations to be largely linked to instrumental advantage such as financial gain or some auxiliary benefit for the offender. The objective of the cybercrime was associated with the motivation in such cases, that is, if the goal of a cybercrime was money, the motivation was assumed to

[115] The "realisation" of the opportunity of crime by the offender was alluded to in the preceding section in Chapter 5.3, and was explored as "intention" (which can also infer motivation). In this thesis, motivation is viewed as a process that starts well before the event of a crime.

be financial gain, a logical presumption as suggested by Hutchings. In Holt's (2013) research on Russian forums, the interactions among actors point towards social processes driven based on the supply and demand of goods and services. It follows, from Holt's view, that offender behaviour models the principles consistent with economic behaviour. The implications of such a view would imply that successful interaction between offenders is predicated on both parties mutually benefiting from the interaction. Broadhurst et al. (2013) noticed that although motivation of cybercriminals is largely reported to be financial, motivations in the broader cybercrime landscape are assorted.

In the research, it was observed that intentions varied and in certain instances did coincide with gaining advantage in some form. While the intention of an action underlies the motivation of financial profit is indeterminate by simply observing online interactions, it may be reasonably inferred. Contrary to "rational" behaviour, certain discussions support behaviour characteristic of altruism, that is, behaviour indicative of selflessness and a concern for others, for example the sharing of files or posting tutorials without asking for a fee or "vouches". In other situations, there was indication that *gaining* trust and reputation was the intention, which could conceivably link to profit as a motivation if a seller relies on their reputation to attract buyers. There was also indication of members justifying certain malicious action. There is often the tendency to view cybercrime as crime driven by monetary reward. The goal of this section is to highlight the different motivations by web forum site members. The findings in Chapter 4 indicated that motivation could be learned through online interactions on the web forum sites, however, as will be revealed in this section, motivations, as inferred based on the discussion content, are diverse and depend on the goals and circumstances of the web forum site member.

The following example indicates that certain crimeware creators may have motivation linked to profit. In the discussion thread below, the [OP] posts their tool called *Calypso Logger* and provides a website link where the tool can be ordered.

> [Topic]: Calypso Logger Version 0.1 100% FUD
> [OP]: [Screenshot of tool] [List of features of the tool]
> How to Order Calypso Logger: Please Visit Website
> Website: http://calypsologger.tk

(Forum E10 Thread #6)

On the other hand, in the next example, the motivation of one crimeware creator does not involve financial profit. In the discussion thread below, the [OP] shows gratitude to other members and, as stated by the [OP], was "inspired" by the other members who have helped to work on their crimeware tool. The motivation to create the tool and release it, in this instance, suggests influence from online peers plays a role. Behaviour that maximises the chance of recognition or acceptance from online peers is one possible motivation in such a case. However, depending on the circumstances of the web forum site member, it is conceivable that the goal to build reputation may potentially be driven by reasons such as profit, as positive reputation among members can influence and improve the success of future dealings in buyer and seller exchanges.

[Topic]: Devil shell v2.0 Released …
[OP]: Here to launch My Devil Shell free, last Version is Devil Shell v2.0. I want to say thanks to [usernames redacted] who always here to help me and inspire me with there ideas and especially [username redacted]
[R1]: This is a sweet shell [tool], and I will be using it a lot. It is rather visually appealing.
[R2]: Yeah, I was about to say the same thing, it is nice looking … it does look nicely coded
[R3-OP]: Thanks guys for appreciating my work ... use new version. Guys like you inspire me to do more work on it.
(Forum A4 Thread #1)

The following example shows one member that may have multiple motivations. The [OP] asks for donations via *Liberty Reserve*, a digital currency service, for providing a service to setup remote access trojans. However, the behaviour by the [OP], specifically the act of providing a free service suggests altruistic-like behaviour. The [OP] may not benefit monetarily in this case as payment is implied to be optional.

[Topic]: Free - Setting up any RAT + Portforward + 0/37 crypt
[OP]: Hey guys I saw a lot of people asking for help over in the RAT section. I can help you guys in setting up such RATs. Cybergate - All versions / DarkComet - All versions / XtremeRat - All versions / Spy-rat - All versions / And portforwarding.

> Donation is pretty much welcome also … when you donate by LR [Liberty Reserve] …
> (Forum C9 Thread #10)

There was also indication that motivation is linked to the gain of reputation or increasing perceived trustworthiness. In the follow example the [OP] posts over 30 hacking tools for download and in their post requests other members to "Rep+" and "Like" the thread, which was also similarly highlighted in Chapter 4.4 as a social dynamic that contributes to the learning process. Revisiting the study by Décary-Hétu and Dupont (2012), it was suggested that perceived trust between web forum site members affected the amount of interactions, that is, a more trustworthy member may encounter more interactions. A strong reputation is beneficial for certain members and one manner in which reputation can be built is through such processes and website forum features that help to quantify reputation. A motivating factor to engage in certain behaviour may be to accumulate one's reputation, which consequently can offer certain advantages to a web forum site member.

> [Topic]: Free - 30+ Hacking pack - Free
> [OP]: Alright guy's I'm releasing my hacking pack, with program's I've collected in the past week or so, I'll be adding more throughout the year. What does this package provide? Well I separated the files, but it contains: Crypter, Bombers, DDoS Programs, RAT's … Darkcomet etc. …, Spamming programs, Website IP attacker, Havij 1.5 + Crack & 50K IP's. [Download link for tool]
> Please Rep+ and Like this thread!
> (Forum H4 Thread #13)

Altruistic-like behaviour is also evident in the next example. In the discussion thread below, the [OP] posts a keylogger tool for download, with no cost required to download it. Interestingly, the tool is provided as a "special release" specific to the web forum site participants.

> [Topic]: Doctor Logger v4.1 - Keylogger/Stealer/Downloader/Binder
> [OP]: DoctorLogger v4.1. Special release for [Web forum site redacted], Keylogger Unreleased 4.1 called DoctorLogger. This keylogger incudes, stealers, a file binder, a icon changer and lots more. [Download link of tool]
> (Forum E10 Thread #7)

There was also indication of behaviour in which there appeared to be no identifiable motivations. For example, as indicated by [R2-OP], it is stated the reason for posting a tutorial as a discussion thread was due to boredom.

> [Topic]: Tutorial - Basic MySQL injection …
> [OP]: Before you say there are already enough tutorials on here, I know. But I plan on making this one of the best on [site name redacted]. If you're looking for SQL injections [website hacking technique], or WAF bypassing [wireless network hacking] please look at the bottom of this thread. [Tutorial provided]
> [R1]: Nice guide …
> [R2-OP]: This is my first tutorial I've ever written. I wrote it out of the blue, cause I was bored.
> (Forum A2 Thread #12)

Observed behaviour also suggests motivations are linked to the pursuit of amusement. In the follow example, the [OP] seeks the help of other web forum site members to hack into a website that is run by a friend. The discussion by the [OP] also indicates techniques of neutralisation (Sykes & Matza, 1957), as the [OP] justifies the illegitimate act of the DDoS attack to be a prank.

> [Topic]: Can someone help me hack a forum on [website name redacted]
> [OP]: My friend has a forum on [website name redacted], and I want to play around with him. And I don't like some of the admins he hired there. Can anyone help me please?
> [R1]: Yes, PM me I can DDoS it. And I could have a crack at defacing it.
> [R2-OP]: Thanks man, I'll PM you in a while. This would be funny …
> (Forum B1 Thread #16)

Motivations are also linked to thrill-seeking behaviour and associated as a game. In the following example the [OP] posts a "challenge" to hack into a website. To prove that members have in fact hacked into the website, the [OP] asks for members to post details of the hacked website that could only be provided if it were actually hacked. The [OP] has posted a list of web forum site members that have successfully completed the challenge.

> [Topic]: SQL Inject Challenge #1 – Easy - Website hacking challenge

[OP]: Very simple, just do the following. Post a picture of the table name(s). Post a picture of the version. Anything else you'd like to post is OK, as long as it has something to do with the thread. Make sure to edit it to where your [Website redacted] name is in the picture. Website [Target website redacted]
Completed:
- [username name redacted] ~ Nice man.
- [username name redacted]
- [username name redacted]
- [username name redacted]
(Forum A3 Thread #19)

There were also cases of web forum site members justifying the act of disseminating potentially illicit information such as a botnet tutorial. In the example below, the [OP] states that they are not liable for the actions that may result from the botnet tutorial posted. This would be a clear example of "denial of injury" (Sykes & Matza, 1957) in which the offender validates an action based on the belief that no one is actually harmed.

[Topic]: Botnet tutorial
[OP]: I am not held responsible for your action. A botnet can be used to keylog computers, capture screen shots, turn on webcam and take pictures, … get passwords, perform DDoS attacks, run commands, open sites, basically anything. I wrote this botnet tutorial. Here we go ladies and gentlemen. Follow the botnet tutorial: [Tutorial provided]
(Forum E5 Thread #3)

Neutralising behaviour in the form of appealing to "higher loyalties" (Sykes & Matza, 1957) was also evident. The [OP] in the below example reveals that the reason for the website defacing tool that they are seeking is to attack sites of "human rights abusers" and justifies their actions are for the greater good.

[Topic]: Any deface tools around?
[OP]: Hi everyone. I'm slightly hesitant to ask but does anybody know of a decent tool for deface. Reason I ask is that as someone with a toddler's understanding of coding, processes etc such a device would at least allow me - until my knowledge on hacking increases - a chance to target sites that are run by human rights abusers etc. Any suggestions, advice, experiences, links would be a big help …
(Forum H1 Thread #16)

5.5 Variations of Targeting

The choice of targets among offenders, and the method in which victims are targeted, is also capricious. Pratt, Holtfreter and Reisig (2010) draw from routine activity theory, as well as self-control explanations, to describe why certain individuals become targets. The broader finding of the study revealed that ostensibly disparate theories such as routine activity theory and self-control explanations do not conflict when explaining victimisation. They also showed that increased online Internet usage increased the likelihood of becoming a victim as, "… greater participation in remote purchasing increased consumers' exposure to fraud targeting and increased their risk …" (p. 207). Similarly, Hutchings and Hayes (2008) identified that individuals who spent more time on Internet activities were more likely to be targeted by motivated offenders. It seems a logical connection that the likelihood of becoming a target increases with further exposure to the situations in which crime may *potentially* occur. Such research has revealed insight into victimisation patterns and supports the applicability of the routine activity theory to certain cases of cybercrime.

From the perspective of offenders, Felson and Clarke (1998) outlined four elements that make a target more attractive in predatory crimes, namely value (associated with the target by the offender), inertia (weight of the item), visibility (how exposed the target is) and access (ease of engaging with the target). Such elements can translate differently in the cybercrime scenario. In the influential paper by Yar (2005) that discusses the relevancy of routine activity theory to cybercrime, the four elements are translated to the Internet scenario. The topic of *value* will be covered in the next section, Chapter 5.6, which Yar (2005) refers to *information* as having worth for offenders. Inertia, as described originally by Felson and Clarke, is moot, as data clearly has no physical weight associated with it, which Yar (2005) links to "size" of data. For example, theft of a large amount of personal private information is greater in size (bytes) and may entail more time during offender-target engagement, as Internet bandwidth is finite. Yar (2005) equates visibility to whether systems are openly connected to the Internet. Lastly, the deployment of security products such as firewalls and detection systems exist to deter and prevent access from offenders. Yar (2005) also raises a relevant point that the offender, through the use of tools, can sidestep these protective measures.

The goal of this section is to provide insight into the decision processes of the offender when selecting victims. The observed web forum site interactions reveal the selection of targets from the perspective of offenders. In the research, there are six common themes that were identified with respect to the selection of targets, namely indiscriminate targeting, the targeting of specific sites or organisations, targeting via an intermediary such as through a botnet, technology focused targeting, and targeting based on specific vulnerable characteristics.

While the Internet has simplified legitimate activities, it has also improved the ease of engaging in criminal activities (Broadhurst et al., 2013), and has also provided a setting for new types of malicious activities to occur. Search engines that are designed to find information and used as a method to navigate the Internet are also employed to facilitate target selection for offenders. There were online interactions that suggest that the choice of targets by offenders were randomly selected leveraging legitimate technologies. In the following example the [OP] lists targets that can be chosen arbitrarily according to the vulnerability of websites through the process of *dorking*.[116] For example, in the first dork below, a Google search query that contains *inurl:"/cart.php?m="* would retrieve sites with the specific property that can be exploited for unauthorised access; such information may be used by offenders to hack into websites.

> [Topic]: Hack Credit Cards - Shopadmins - Exploits - Dorks
> [OP]: 1: google dork :--> inurl:"/cart.php?m="
> target looks like :--> http://xxxxxxx.com/s...cart.php?m=view
> exploit: change cart.php?m=view to /admin
> target with exploit :--> http://xxxxxx.com/store/admin
> Usename : 'or"="
> Password : 'or"=
> 2: google dork :--> allinurlroddetail.asp?prod=
> target looks like :--> xxxxx.org (big letters and numbers)
> exploit :--> change the proddtail.asp?prod=SG369 whit fpdb/vsproducts.mdb
> target with exploit :--> www.xxxxxx.org/fpdb/vsproducts.mdb
> 3: google dork :--> allinurl: /cgi-local/shopper.cgi

[116] A *dork* is a technique used by cybercriminals to identify vulnerable computers, servers and websites on the Internet using Google search queries.

target looks like :--> http://www.xxxxxx.co....dd=action&key=
exploit :--> ...&template=order.log
target with exploit :--> http://www.xxxxxxxx.....late=order.log
(Forum C3 Thread #2)

On the topic of crime prevention, Ekblom (2014) has suggested that certain "spaces" could be constructed in a manner to deter crime. Perhaps in practice a similar approach could be extended to the virtual environment of the Internet, such as filtering or disallowing such search queries.

The selection of targets in certain cases was not completely random. The [OP] in the following example states they are engaging in DDoS attacks and requests for other members to post possible targets. A selection of targets is listed separately that are easy and difficult to attack. By listing such sites, it may direct other web forum site members to attack the listed sites. Interestingly, the [OP] suggests not to target particular sites, for example, "government" websites.

[Topic]: … Powerful DDOS Botnet … Takes down major sites … Challenge me? …
[OP]: Hey, so I got that powerful DDoS Botnet. Real powerful. I'm going to make here a list of sites that can and can't be DDoSed. I'm performing DDoS tests for 1-3 minutes. So, post your host and know if it can be DDOSed. You may ask for major websites but please don't ask to DDoS Google\Facebook\PayPal\government sites. Also don't ask to attack weak targets, only strong ones. Also don't ask to attack Cotendo\Akamai servers because they have multiple IPs for each country so it's useless. …
Sites that CAN be attacked:
1) http://www.m[redacted]m.net [Large company website]
2) http://www.m[redacted]t.net/ [Large company website]
3) http://www.a[redacted]s.com [Online shopping website]
4) forum.s[redacted]s.com [Car enthusiast website]
5) http://www.m[redacted]s.com [Photo blogging website]
6) http://www.p[redacted]n.com/ [Online shopping website] …
Sites that CANNOT be attacked:
1) http://www.p[redacted]c.com/ [Banking website]
2) battlelog.b[redacted]d.com [Gaming website]
(Forum A9 Thread #4)

Similarly, the following example shows a discussion thread that contains a list of vulnerable sites. Such discussion threads conceivably entice other members to engage in malicious activities towards the listed sites.

> [Topic]: Vulnerable Sites!
> [OP]: Hi, this is my first post. I will post some vulnerable sites for you.
> http://www.j[redacted].de/jugendarbeit/event.php?id='138 [Large company website]
> http://www.d[redacted].de/de/event.php?id='100 [Small business website]
> http://www.f[redacted].de/event.php?id='1364 [Online shopping website]
> http://www.a[redacted].co.uk/events/event.php?id='408 [Small business website]
> http://i[redacted].co.uk/event.php?id='13 [Small business website]
> http://www.i[redacted].co.uk/event.php?id='12 [Large company website]
> (Forum C3 Thread #18)

Wortley (1998) suggested that there are situations that can prompt criminal behaviour. The listing of sites vulnerable to hacking and DDoS attacks may act to focus the outcome of a criminal response (for the case of the already motivated offender that seeks any target). Such listed sites are more likely to be targeted by offenders for the reason that they are publicly listed and implied as weak potential targets.

There was also indication of offenders selecting specific targets on the Internet. The [OP] in the following example provides explicit instructions on how to hack the Discover credit card website.

> [Topic]: Hack Discover … CVV + Available Balance … 2013 …
> [OP]: How to hack Discovery. First step, need to have Discovery logins [list of emails of Discovery credit card customers]. Should spam [via email] accounts from Discover. I have some here I have got from spam, and I give now free. [Details provided]
> [R1]: Thank you! …
> (Forum C4 Thread #19)

Target selection was also based on certain industry sectors, for example, online financial and banking institutions were common targets listed on the web forum sites. In the

discussion thread below, the [OP] states they have a list of phishing pages[117] available that they are openly distributing. Such pages can be used along with crimeware to siphon funds from victim's bank accounts.

> [Topic]: 2012/2013 Banks phishing pages
> [OP]: Hello […] I'm here to learn and to help our members too, so here are the latest banks phishing pages also called scam page:
> .::SCAM PAGE::. _____.:Description Of Scam Page::.
> (American Express) ++++++++++++ American Express Bank - Full Info
> (American Express CC) ++++++++++++American Express Bank - Card Info
> (Discover) ++++++++++++ Discover Bank - Full Info
> (HSBC) ++++++++++++ HSBC Bank UK Version - FULL Info
> (RBS) ++++++++++++ The Royal Bank of Scotland - FULL Info
> (Royal Bank) ++++++++++++ RBC Royal Bank Canada- FULL Info
> (PNC) ++++++++++++ US PNC Bank - FULL Info
> (Chase) ++++++++++++ US Chase Bank - FULL Info With Email Access
> (CIBC) ++++++++++++Bank CIBC Canadian Bank Full info
> All this listed banks are available in PM. All I need is your rep & thanks.
> [R5]: Can you send me 2012/2013 Banks phishing pages?
> [R6]: Can you send me? I will rep you. Thanks for sharing the post, nice share.
> (Forum B1 Thread #4)

To view a sample collection of targets generated from the use of the *Zeus* crimeware by cybercriminals, refer to Case 4 below. The full collection consisted of 196,000 sites that were targeted. From the sample, only ten random sites were extracted for illustrative purposes. As shown, it appears the ten sites are either banks, credit unions or related to financial services.

Case 4: Instructions sent by cybercriminals using Zeus crimeware

---

A random sample of ten targets (from over 196,000) sent through ZeuS botnets worldwide are listed. The random selection primarily consisted of banks and financial institutions. Such cases reveal that botnet operators are using ZeuS botnets with the intention to steal information for the purposes of siphoning funds from individual's bank accounts.

https://core.cedacri.it/*/LogonStep* [Cedacri Group – Banking related]

[117] *Phishing pages* are websites that appear to be genuine websites, generally banks and financial institutions, which aim to deceive victims. Controlled by cybercriminals, these webpages attempt to solicit personal private information from victims through social engineering techniques (US CERT, 2014).

https://businessonlinebanking.ebanking-services.com/Nubi/signin.aspx
https://*mybank.alliance-leicester.co.uk/*
https://ibank.barclays.co.uk/olb/x/LoginMember.do
https://home.cbonline.co.uk/login.html*
https://extranet.banesto.es/*/loginParticulares.htm
https://www.unicaja.es/PortalServlet* [Unicaja – Banking related]
https://www.moneybookers.com/app/login.pl*
https://e-access.compassbank.com/bbw/cmserver/welcome/default/verify.cfm
https://online-business.lloydstsb.co.uk/customer.ibc [Lloyds Bank]

Note: Refer to Chapter 3.6 (Table 4) for further details on the source of the data.

The targets, and the method in which offenders target them, are temporary and constantly changing. Eck (1993) suggested that the target and methods of crime could be displaced. Crime can be displaced based on target where offenders move from one type of target to another, in addition offenders can change their modus operandi but repeatedly target the same victim.

On the web forum sites, targeting through the use of botnets, as proxies, was evident. The following three examples show the use of botnets, as a tool, to engage in cybercrime. The next discussion thread mentions the use of using botnets to inflate the statistics of *YouTube* views.[118]

> [Topic]: YouTube View Booster - Bot to give you views for YouTube accounts
> [OP]: Hey guys. First release - to public - so hope you like it. This is a YouTube view booster bot, which is used to give your videos views. Proxy support may come if people ask for it
> [Screenshot of tool] [Virus scan of tool] [Download link of tool]
> (Forum H5 Thread #4)

The following example is similar to the previous, however the [OP] inquires about the use of botnets to increase traffic to their *Livestream*[119] website. In such cases, it is the content service providers as well as the advertisers that provide payouts based on the number of

[118] Money can be earned by *Youtube* content creators by showing advertising. The more viewers that open or view a Youtube video, the more income that is generated for the content creator. A common way to make money among cybercriminals is to create fake Youtube accounts for the purposes of fraud. Botnets are used to impersonate real Youtube visitors. This fraud is not specific to Youtube and is found on other sites that provide a similar service.
[119] *Livestream* uses a similar revenue generation format as Youtube.

views that are defrauded. To clarify how the fraud occurs, crimeware is used to build botnets, and it is the botnets that mimic fake "visits" to such sites.

> [Topic]: Best setup for traffic
> [OP]: Hey, just wondering if I'm approaching this correctly and looking for advice. I'm looking to boost popularity of some livestreams and was looking into the potential of using a botnet to help boost views, to enable me to earn money from my stream. The more views I have on the live stream, the more potential for "real" visitors to watch the stream and ultimately it looks less suspicious as it gains popularity. Is there a loader available currently with the potential to send zombies [botnet traffic] to my stream silently? Would I be better off using a RAT to do so? I would rather use a much more basic smaller bot …
> [R1]: I'd recommend a simple loader or RAT.
> (Forum F4 Thread #11)

Interestingly, there are specific bot kits designed to inflate traffic for specific websites. Essentially, such tools are specifically designed to target a defined website or online service. In the follow example, the [OP] distributes a bot tool designed to inflate *ADF.ly*[120] traffic. *ADF.ly* website links can contain advertising that generates revenue similar to *Youtube* and *Livestream*.

> [OP]: Description:
> * Name: ADF.ly BOT
> * Version: v152 build 17s
> Features:
> * Cool GUI.
> * Supports 5 links to avoid ban
> * Supports proxy.
> * You can import multiple proxies from a text file.
> … [Screenshot of tool] [Download link]
> [R4]: Nice Bot ... got it working. Lets see how much I earn in a day. I will post it soon, the stats.
> (Forum H5 Thread #5)

[120] *ADF.ly* is a URL shortening service that generates income through advertisements that are shown to a visitor. When an ADF.ly website link is clicked by an individual, a small amount is paid to the creator of the ADF.ly link.

Choo (2011a) suggested that botnets can be used to propagate different types of malicious activities such as bank phishing, automated activities, for example the *Youtube* and *Livestream* fraud listed previously, as well as host illicit data. In such scenarios, the target website of a botnet is considered the objective of the cybercriminal. However, the bots itself, which compose the networks of compromised computers, are also targets. Botnets are frequently highlighted as an intermediary to target victims, but the bot-infected computers are also victims. In Case 5 below, examples are provided based on real-world botnet data, generated from the *Zeus* crimeware, stolen from bots. The full data source consists of 1,214 victims, however only three victims were randomly selected for illustrative purposes.

Case 5: Stolen data collected from cybercriminals using Zeus crimeware

---

An example of stolen data captured by cybercriminals using the ZeuS botnet are shown below. Three examples of victims (out of 1,214) were randomly selected from Australia. For Victim 1, the email contacts of the victim were captured by the cybercriminal. For Victim 2, the PayPal balance of the victim was stolen along with the user id and password of the victim. For Victim 3, personal messages were captured from a victim's online session on a social networking service. The stolen data demonstrates different forms of data being captured by cybercriminals through ZeuS infected bot computers. The stolen data shows the multiple purposes that botnets provide for cybercriminals as data can be stolen from bot infected computers, with the owner of the compromised computers as victims, and can also be used to propagate other attacks when used as proxies.

From Victim 1:
a[redacted]n@vanmildert.com
a[redacted]j@members.ebay.com.au
a[redacted]5@gmail.com
b[redacted]709rdt@members.ebay.com.au
c[redacted]49@hotmail.com
c[redacted]gp@tpg.com.au
g[redacted]cy@westnet.com.au
y[redacted]2k7@googlemail.com
h[redacted] mods@gmail.com

From Victim 2:
Grabbed data from: https://www.PayPal.com/ … [login id and password redacted]
Account Limits: View Limits
PayPal balance: $439.73 AUD
Currency converter
Available balance in AUD (primary): $439.73 AUD
Total balance (all currencies, available and pending) converted to AUD: $439.73 AUD

From Victim 3:

Site: http://[redacted].com.au/inbox.php [Australian LGBT community forum]
User input: [username redacted] u wanna have fun next week? … can send via mobile 04[phone number redacted]

Note: Refer to Chapter 3.6 (Table 4) for further details on the source of the data.

The selection of targets, by web forum site members, was also determined based on technological platform. There was indication that certain technological characteristics such as mobile devices used by potential victims were the target. In the next example, the [OP] has posted crimeware that target mobile devices that use the *Android* operating system.[121] Such crimeware tools can be used to steal data from mobile smartphones and tablets that use an Android operating system.

> [Topic]: Android trojan info stealer - …
> [OP]: [Screenshot of tool]
> [Download link of tool]
> (Forum C9 Thread #14)

The following example reveals discussion by the [OP] of whether a remote access trojan can be used on an *iPod* touch,[122] a type of mobile technology.

> [Topic] Is it possible to use a RAT on an iPod touch?
> [OP] I am an extreme new fag with this stuff and I want to learn. Is it at all possible to run a RAT on an iPod? I have very little knowledge on RATs. My extent of knowing how to use them is downloading them onto another device and my computer, and controlling the device but I have never got it to work. Could someone teach me please?
> [R3] Yes, you can RAT phones. I don't think there are any public RATs out … the bigger problem would be getting them onto the phone.
> (Forum D3 Thread #18)

Targeting was also selected based on the vulnerable characteristics of the potential victim. Radianti, Rich and Gonzalez (2009) examined black markets where exploit code was traded

[121] *Android* is a mobile operating system that is primarily used in smartphone and tablet computers.
[122] *iPod* touch is a digital device with Internet connectivity capabilities.

for potential illicit purposes.[123] Similarly, Maurushat (2013) explored the different ways in which security exploit code were disseminated online, which also included markets that specifically distributed zero day[124] exploits. The market for exploits and vulnerabilities is distinct from crimeware, and outside the scope of this thesis. However, discussion content relevant to exploit code was observed in the crimeware web forum sites. It should not be overlooked that certain crimeware are dependent on exploits (for example, specific exploits found in exploit kits) that take advantage of vulnerabilities.

The following two examples highlight the distribution of exploit code, specific instructions on how to take advantage of a security flaw. The first example is an exploit related to *MyBB* which is a platform used in many web forum sites.[125] The [OP] refers to the exploit as a "0day" denoting that the security vulnerability has been identified relatively recently.

> [Topic]: 0day MyBB exploit SQL injection for profile albums.
> [OP]: Code:
> ##
> # Exploit : Profile Albums MyBB plugin SQL Injection
> # Date: 17.10.2012
> # Software Link: http://mods.mybb.com/view/profilealbums
> ##
> # [redacted] :albums.php intext:"powered by Mybb"
> ##
> # The vulnerability exist within albums.php :
> #<?
> # /*Line 69*/ $aid = $mybb->input['album'];
> [Part of exploit code redacted]
> (Forum H7 Thread #10)

[123] It is important to delineate "vulnerabilities" from "exploit kits" or "exploit code" although they are often used interchangeably. Vulnerabilities, sometimes referred to as exploits, are unwanted or unknowing weaknesses in systems connected to the Internet. Exploiting, via an exploit 'software' kit or code, takes advantage of a vulnerability.
[124] *Zero day*, or 0day, is a vulnerability that is revealed before it has a chance to be addressed and fixed.
[125] The full technical details of how exploits work will not be covered in this thesis.

The following example is of a discussion post of exploit code posted by the [OP] that relates to a security vulnerability of the *Opera* web browser. Such details can be used by cybercriminals when creating exploit kits that target victims who use the Opera web browser.

> [Topic]: Opera SVG Use-After-Free
> [OP]: Opera appears to suffer from a SVG use-after-free vulnerability.
> <svg xmlns="http://www.w3.org/2000/svg"
> xmlns:xlink="http://www.w0.org/1999/xlink">
> <g id="group">
> <defs>
> <clipPath id="clip-circle" clip-path="url(#clip-rect)">
> </clipPath>
> <clipPath id="clip-rect">
> </clipPath>
> </defs>
> [Part of exploit code redacted]
> (Forum C3 Thread #17)

Lastly, another form of targeting was evident through a process known as doxing.[126] The following discussion thread explains the doxing process. Doxing is typically used to reveal private information on a specific individual for malicious purposes such as blackmailing and in other cases it is used to create nuisance. Norris (2012) described doxing as a type of online vigilantism, which in recent years has largely been associated with ideological motivated hacking activities. The techniques of doxing do not involve the use of crimeware, however doxing related discussions were common in the web forum sites examined.

> [Topic] Doxing Tutorial - Advanced
> [OP] Doxing, is the term used for the process of gathering personal information on a slave or target [any individual]. Although this does commonly take place over the

[126] *Doxing*, which originates from 'document tracing', is a method used to reveal personal private information on an individual to the public. Examples of information include a home address, financial details, and other personal information. The act of publicly disclosing personal information occurred as early as the 1990s on earlier online communication platforms such as Usenet.

Internet, this isn't always the case. There are many methods of doxing, and various tools available over the Internet.
[Tutorial on doxing provided]
(Forum A2 Thread #5)

5.6 Value

A primary assumption of the rational offender is the value the offender attaches to certain needs (Clarke, 1997). Cohen and Felson (1979) suggested that the attractiveness of a target for an offender depended on four qualities, one of which included value.[127] One would assume the concept of value to be associated with money or a form of tangible good. In the cybercrime scenario, Hunton (2009) expressed that it was electronic data that had a perceived value for cybercriminals. The question then arises, if offenders are maximisers,[128] then what is maximised? As revealed in this chapter, and in Chapter 4, examples were presented that showed that the choices made by certain web forum site members were consistent with the precept that individuals were ultimately self-seeking opportunists. Depending on the discussion thread, the element maximised, in other words the "object" of value, varied based on the situation and needs of the web forum site member. The seven items of value observed in the web forum sites are listed (see Table 6).

Table 6: Developing the concept of value

Value	**Examples**
1. Money	E-currency, access to monetary funds
2. Software (crimeware)	Packaged tools, applications, code
3. Knowledge	Techniques, vulnerabilities
4. Skill	Specific skills, providing skills for a service
5. Stolen data	Website login credentials, credit card numbers
6. Trust and reputation	Reputation among offenders
7. Access to other offenders	"Knowing the right people"

[127] The other three of four qualities pointed out by Cohen and Felson (1979) include physical visibility, access and inertia of the target that work contrary to the actions of the offender (for example, a door with multiple locks).
[128] The notion of *maximising* behaviour should be interpreted simply meaning to increase or accrue some element to the greatest possible amount. The simplest example is profit, however it can broadly include other factors such as reputation or crimeware. Refer to Table 6 for examples in the study.

The transfer of money through wire transfer or e-currency was common in interactions where an exchange occurred. In the following discussion thread, the [OP] makes an open request to purchase stolen *PayPal* accounts and prefers the transaction be done through a *Western Union* money transfer. In this particular case, the items of value would be money and the stolen *PayPal* account data.

> [Topic]: I want to buy PayPal balance - hacked / legit
> [OP]: I want to buy PayPal balance 100$ which may be hacked or legit. I will pay you through Western Union! Let me know your prices!
> [R1]: I have a lot of PayPal accounts for UK, US or EU with bank & credit card details but no balance. You can send from bank. PM me if interested.
> [R2]: I got a US PayPal with $111 balance, not logged in since 2009. Will give you it to me first then pay me since I'm new? PM me.
> (Forum C14 Thread #1)

Similarly, credit card details also have intrinsic value. The [OP] in the following example seeks to acquire stolen *American Express* and *Visa* credit card numbers.

> [Topic]: I want to buy AMEX, VISA non VBV[129] [Verified by Visa] …
> [OP]: I'm trusted I need a Visa or AMEX High balance non VBV via Visa. NO dead or used ones PM me if you have. I will buy more than 20 per day. Payment will be made when transaction done.
> [R1]: I have Visa, MasterCard … and AMEX … PM me if interested.
> [R2]: PM me your Yahoo contact details and I'll give you a test.
> (Forum C14 Thread #2)

In certain cases, the primary currency (money) was converted into a secondary form of currency. In the following example, fraudulent electronic gift cards are sold. Assuming the source of money was the result of cybercrime, such activity would reveal a basic form of money laundering in which the proceeds of crime are disguised as coming from legitimate sources. The item of value in this case would be the electronic gift cards. The [OP] has requested the transaction to be done through *Liberty Reserve* or *Western Union*.

[129] *VBV*, or Verified by Visa (VbV), is a system used by Visa to make transactions more secure. A password is registered to a specific credit card on the Visa system, which is required for authentication when a Visa transaction is made online.

[Topic]: Clinique.com egiftcard and Aveda.com egiftcard
[OP]: I have some Aveda.com egiftcard and Clinique.com egiftcard, they can be used to shop 24/7 at Aveda.com and Clinique.com. If you need, please contact me for information on prices. You will save when you buy more. Yahoo: [Yahoo ID redacted]. I accept payment via Liberty Reserve or WU [Western Union].
[Screenshot provided of gift card balance]
[R1]: I'm interested in doing this deal.
(Forum E11 Thread #8)

Monetary currency also came in the form of e-currency such as bitcoin.[130] In the following example, [R3] makes a reference to bitcoin and advises the [OP] that they would have to pay for a crypter using such e-currency. The item of value in this case would be the crypter tool as well as the bitcoin e-currency.

[OP]: I'm in need of a FUD crypter. Can anyone help and maybe explain a little?
[R1]: I can help you ... email me.
[R2-OP]: At today's date, I don't have any money, so if you're after my money by saying you can help. Sorry, if I had money. I would have paid.
[R3]: Dude if you don't have a single bitcoin to spare for a FUD crypter, then good luck.
(Forum D3 Thread #9)

However, in certain interactions currency was not the only item of value used to ensure exchanges took place. For example, the [OP] in the following discussion thread draws on their reputation and "vouches" as a way of showing they are knowledgeable in setting up remote access trojans. Reputation also functions as an indirect form of value to certain web forum site members.

[OP]: I will setup any RAT for you like Darkcomet, Cybergate, Blackshades, etc. As you can see from my reputation report and vouches below, I have been pretty successful in setting up RATs. I will also crypt it and give you installs.
Here are my packages:
Package 1: Setup any RAT. Port Forward. Give you 20 slaves. Crypt it - Not necessary to be FUD. Price: $7.

[130] *Bitcoin*, is a digital form of currency that was first introduced in 2009. Digital currency such as bitcoin has been controversial as it has been often associated with cybercrime. It is an unregulated decentralised currency that cannot be traced.

Package 2: Setup any RAT. Port Forward. Give you 10 slaves. Price $5. Misc. Information.
I accept payments in PayPal and Liberty Reserve. Other Payment processors can be discussed.
(Forum A13 Thread #1)

Exchanges between web forum site members also involved illicit services. In the next example, the [OP] states that they are willing to trade their install service, in other words the [OP] is offering to create new bots, in exchange for crypting services. The items of value would be the services provided by the two parties in the transaction. This also supports that certain members have specific skills and are specialised.

[Topic]: Trading FUD service - 1 week update
[OP]: … With each crypt I do 5 installs, and u choose the country that you want.
[R1]: I can crypt your file to stay FUD for one week for some installs …
[R2]: Contact me bro, I will help you.
(Forum A14 Thread #2)

There were also cases of one-to-one trades in which the control of bots were exchanged with other bots. The [OP] in the following example states they are seeking "installs for installs" in other words suggesting that they want to trade the control of compromised computers.

[Topic]: Trading installs for installs / bots for bots … i4i
[OP]: Hi … I am willing to exchange installs for installs. If you are interested in this, shoot a PM my way or place a comment here, and we can work something out. That's all for now.
[R1]: I have 3 or 4 slave in my Cybergate [botnet]. If u like to have them just send me PM …
[R2-OP]: Sure thank you! I will throw you a PM now.
(Forum H8 Thread #7)

Most interactions of a transactional nature did indicate the straightforward exchange of money (or e-currency) for a good or service. In certain interactions, it was clear that the medium of exchange was the same. For example, it was the control of compromised computers, or botnets, that was swapped in the previous case. Although money was

commonly used, whether in the form of a wire transfer or e-currency such as bitcoin, the web forum site markets show characteristics suggestive of "international trade" in which goods and services are exchanged (rather than money).

Specific skills, another item of value, also played a part in transactional exchanges. The capability to create custom tools, such as a remote access trojan or crypter in the example below, is offered for a price. Interestingly, the [OP] asks for money up front and the rest after the task is complete. Transactions did not always involve one-time payments and interactions.

> [Topic]: Custom coding, RATS, Cryters and more.
> [OP]: I will build you a custom RAT or Crypter with source code starting at $1500 USD. Coded in Delphi 7 [programming language]. I accept Liberty Reserve or Western Union with $500 to start project, and $1,000 upon complete. Complete time is 1-2 weeks. To get a free estimate, email the details of what features you want to [email redacted] …
> (Forum F4 Thread #1)

Similarly, in the next example the [OP] provides prices for custom tool services, as well as discloses a detailed price break down for each type of tool. The prices shown vary depending on the type of crimeware suggesting certain crimeware may have more value than others.

> [Topic]: Need custom coding?
> [OP]: Hello friends, I'm doing custom coding
> Binder - Price: $30 - Estimated time: ~1 day. Crypter - Price : $50 - Estimated time: ~1 day. Spreader - Price: $100 - Estimated time: ~5 day. FTP Grabber - Price: $400 - Estimated time: ~15 days. Form Grabber - Price: $800 - Estimated time: ~15 days. Password Stealer - Price: $300 - Estimated time: ~10 days. Rootkit - Price: $200 - Estimated time: ~10 days. Ransomware - Price: $500 - Estimated time: ~10 days. Keylogger - Price: $200 - Estimated time: ~10 days. R.A.T - Price: Min. $1000 - Estimated time: ~50 days …
> Payment Methods: Liberty Reserve - Western Union - PayPal
> To get a free estimate, email the details of what features you want to [email redacted]
> (Forum F5 Thread #3)

5.7 Conclusion

Crime scholars may consider the topic of crimeware as rather esoteric. It is considered a point of interest in computer security, a very disparate field of study. However, recognising the patterns associated with crimeware and the relevant processes are helpful to identify how cybercrime is committed, the offenders involved and also when considering crime prevention strategies.

The web forum sites revealed different types of crimeware being developed, distributed and used among members. It was clear certain crimeware tools were developed for the sole purpose of engaging in cybercrime. Criminal innovation was also manifest with the continual development of new crimeware tools. In certain cases, a glimpse into discussions pertaining to the development of crimeware revealed members would post early iterations of their crimeware tools, which were continually updated, and in certain cases involved multiple actors working together. As older tools became out of date, due to lack of effectiveness, new crimeware was developed. Intention could also be inferred based on the design of the crimeware. It was apparent that certain tools were designed for malicious use, as great effort was taken to conceal its activity when operative. It was also found that web forum site members used tools, originally designed for legitimate use to protect systems, in order to commit illicit hacking activities. Such accounts expose the contradictory effects of software with features that are fundamentally designed to hack websites and online systems.

The motivation of participants in web forum sites was, in certain cases, linked to instrumental benefit, however this did not equate to financial gain in all cases. The various dealings did involve some exchange of "currency", however did not always equate to money as crimeware, stolen data, services based on a unique skill and even botnet access were transferred. Trust building also appeared to be important for certain members as a member's reputation was taken into account when making opportunistic decisions. The different crimeware and cybercrime techniques revealed different typologies of target selection. In many instances, targeting was non-discriminate as "weak" less-protected websites and servers appeared to be arbitrarily selected and pointed out openly in

discussion threads. Additionally, the cybercrime activity that could be inferred from the discussion was largely *asymmetric* in which a single actor has the ability to target multiple sites with little effort (Wall, 2014). The routine activity theory suggests that vulnerable targets are more susceptible to crime, and this certainly coincides with the findings in this chapter.

Chapter 6: The Macro Perspective

> We can't impose our will on a system. We can listen to what the system tells us, and discover how its properties and our values can work together to bring forth something much better than could ever be produced by our will alone.
>
> *~Meadows*[131]

To recap, the investigation in Chapter 4 focused on the social dynamics occurring within the web forum sites. It was revealed that online behaviours involved online interactions characteristic of learning. The observed interactions indicate knowledge, skills, and preferences were acquired through social processes among web forum site members. It was the social interactions between offenders that were the primary point of investigation. Chapter 5 explored online offender interactions driven by the pursuit of gain. In certain instances, the underlying motivations of offenders were inferred as decisions that maximised individual choices. These varied depending on the needs, capabilities and the situation of the offender.

In addition to examining the social dynamics occurring within crimeware communities, it is important to consider crimeware from the paradigm of broader social structures. Understanding the role of crimeware relative to the wider cybercrime landscape and society presents a more holistic investigation. This chapter will examine the macro sociological aspects of crimeware, that is, it explores the implications of crimeware, and online communities associated with crimeware activities, in relation to other groups in society. Wall (2008, p. 26) stated that it was necessary to separate rhetoric from reality before ascertaining knowledge in cybercrime research. A common rhetoric is the depiction of cybercrime as cases of hacking incidences occurring over the Internet and the success of crime prevention approaches measured by the number of arrests and prosecutions made. The reality is that crimeware is a multifaceted topic that concerns the larger social

[131] Quoted from *Thinking in Systems: A primer* by Meadows and Wright (2008).

ecosystem.[132] This chapter will concentrate on the topic of online communities involved in crimeware activities from a macro social context, which contrasts with the focus on individual agency that is the emphasis in Chapter 4 and, to some extent, in Chapter 5 that focused on interactions of a transactional nature involving smaller groups. Relevant themes examined in this chapter include the function of crimeware communities within society, the way in which law is perceived among stakeholders affected by the criminalisation of crimeware intended to deter cybercrime, and crimeware communities as social systems within society.

Drawing from the macro view of the larger social ecosystem, society is also viewed as the consequence of larger social process in which particular dominant values conflict or clash at the expense of lesser dominant values.[133] This view contrasts with the normative view in which crime is seen as a violation of social norms, which in certain cases are denoted as criminal as declared by the law. The focus of this chapter is on the interactions between groups in society and the processes in which certain values influence or prevail over others.

This chapter will also investigate the relationship between law and crimeware. There will be an emphasis on offender perceptions on the legality of their activities. It will also introduce state jurisdictions, underlining substantive laws, that have implemented measures to control, in principle banning, tools used for the purposes of crime.[134] The challenges to criminalise certain software used for crime are covered, as well as conflicts of interest that have arisen due to criminalisation. Cybercrime discourse attributes ineffective crime control on the Internet to be a result of a lack of cybercrime legislation in certain jurisdictions and difficulties in cross-border cooperation by law enforcement (Broadhurst & Chang, 2013). Society has responded by introducing "rules", e.g., legislation, that aim to prevent cybercrime, which, arguably, has been limited in its effectiveness as software linked to cybercrime continues to pervade the Internet. In light of this, the research suggests

[132] The *larger social ecosystem* perspective is the view of society as a community of different parts of society interacting as a system, which is the underlying focus of Chapter 6. This perspective originates from the functionalist approach introduced by classical sociologists such as Emile Durkheim, Robert K. Merton and Talcott Parsons.
[133] Refer to Chapter 2.10, specifically on views from Marx and Weber.
[134] Note that only state jurisdictions with relevant laws up until 2014, when this thesis was drafted, are mentioned in this chapter.

a mutually dependent relationship[135] exists between the actors that engage in cybercrime, via crimeware, and those with the objective to mitigate such activity. This relationship between crimeware communities with other groups in society such as crime responders is investigated. For example, the actions taken by cybercrime responders are in certain cases anticipated by offenders subsequently influencing offender behaviour and tactics that can work against the original objective to reduce cybercrime.

It is generally acknowledged that the presence of malicious forms of software is undesirable. It is also clear that the usage of certain software by cybercriminals is adverse when it is directed for the actions of crime. Hunton (2009, para. 38) stated that malware is often used as an attack vector that can be technically intricate and, for some illegitimate objective, targets a device. In spite of such activities linked to the use of malware, the online virtual settings where software potentially used for malevolent purposes is *discussed* and propagated can have a constructive purpose in society. The functionalist question then arises, "How can something that contributes to crime also be useful?" Describing the state of crime prevention, Ekblom (1997) observes that *no matter how fast we run we stay at the same place* using the example from *Red Queen's game*.[136] There is a futility as criminals continually adapt to new crime prevention measures making them ineffective, which is the main challenge for effective crime prevention as Ekblom underlines. Ekblom (2000) also remarks that this response by crime prevention may be responsible for altering offender behaviour and their capacity to commit crime. This chapter will answer this question beginning with the exploration of the constructive function of cybercrime and online crimeware communities that subsist in society. The idea of activities associated with cybercrime having an important function in society may seem paradoxical, as crime is a construct that is viewed as an aspect of society that should be, more or less, removed. Elazari (2014) illuminates this point well using the immune system as a comparison: nefarious actors and activities on the Internet may be a necessary evil as, "they make us sick, but they also find those hidden threats in our world, and they make us fix it" (para. 3). Cybercrime has generated an industry of crime prevention providing jobs in both the public

[135] Drawing from systems theory, a complex adaptive system stresses the diversity of the system and its mutually dependent parts that are also able to change and adapt (Holland, 1992).
[136] The 'Red Queen Hypothesis' was first put forward in van Valen, L. (1973) A New Evolutionary Law. *Evolutionary Theory*. Vol. 1, pp 1-18, as cited by Ekblom (1997).

and private sector. Additionally, malicious activity linked to crimeware is among the reasons that have driven the advancement of technology, although more plausibly as a reactionary response to safeguard systems that interface with the Internet. Without the demand to implement such protective measures, the Internet would be arguably less secure and unsafe. To clarify, the position on crime posed is that there are aspects of cybercrime activity that contribute to the functioning of certain groups, institutions and larger society, a view originally proposed by Durkheim (2013) who believed that crime played an important part in the social order.[137] To reiterate Durkheim's key point that was introduced in Chapter 2.10, deviance in society is unavoidable and expected, and not every person prescribes to the collective sentiments of society. On Durkheim's view between deviance and crime, it was stated that, "the only common characteristic of all crimes is that they consist ... in acts universally disapproved of by members of each society... crime shocks sentiments, which, for a given social system, are found in all healthy consciences" (Durkheim, 1933, pp. 70-110). In other words, crime is a consequence of the violation of collective sentiments.

This chapter also examines the ambiguous nature of crimeware tools. It is a topic that lacks "social consensus" on whether the creation or access to such instruments is right or wrong, particularly among Internet security professionals in the private sector focused on protecting users. Whether crimeware is adverse for society or a problem for certain groups is discussed. Since the emergence of the Internet, online-based communities where individuals congregate to discuss topics such as malware and hacking have formed. Holt (2013) identified the shared norms and values within such communities where deviant and criminal malware activities took place, alluding to the view that such communities are a distinct subculture. With a deficiency of empirical research on such communities, there continues to be a lack of knowledge as it is currently recognised that certain software is developed for nefarious use, but little is known about the communities that propagate them. This paucity of knowledge of the inner workings of malware, botnet and hacking communities has created social uncertainty. Actions taken by authoritative institutions, through policy and legislative measures, consider crimeware as morally wrong and for this

[137] Durkheim developed the idea of deviance playing a necessary function in society in his book *The Rules of Sociological Method*, which was first published in 1895. A 2013 re-print of the 1895 publication is cited in the text above, which contains additional work from Durkheim.

reason has progressively become *more* criminalised among jurisdictions. However, the subject of software linked to crime as a technological development in society, as opposed to a strictly criminal invention, and the ramifications of preventing its circulation and use requires further clarification. Important features relating to its ambiguity is an underlying theme that is raised in this chapter.

Blunden and Cheung (2014) made the interesting observation of seemingly constructive organisations and institutions in society, such as the media as provided in their example, unintentionally thwarting others from performing their duties. For instance the *exaggeration* of a particular crime by the media influences public opinion that over emphasises its importance. Groups and institutions do not act separately and are interconnected. Notably, the offenders who engage in cybercrime are inevitably influenced by the responders aimed at stopping them. As Ekblom (1997) predicted, there is an arms race in cybercrime, namely between the offenders committing crime and those aimed at stopping crime.

The purpose of this chapter is to introduce these overarching themes and issues. The themes covered in this chapter will rely on both interviews with crime responders with a selection of key examples from the web forum sites.

6.1 Law and Perceived Criminality

Necessary to ensure the stability of society, Black (1976) suggested that the amount of law in society had an inverse relationship with social control (handling of crime); an increase of law reflects the lack of effectiveness of social control measures. A simplified interpretation of Black's observation would be law existing where other methods of social control are absent. This explanation could describe the increasing number of jurisdictions that have criminalised software used for the purpose of cybercrime, as alternate approaches of social control do not exist.

The often-raised argument for criminalisation is its legitimacy. A complex issue in society has been the ongoing debate of deciding what should be prohibited and punishable.

Common examples include the criminalisation, and in certain cases control through regulation, of guns and instruments used as tools. The attributes of guns can be comparable to that of crimeware. Guns are invented to inflict harm and are availed by both criminals and those with legitimate purposes, and this resembles certain crimeware that are designed to permit malicious actions in the online environment that are used for illegitimate and, supposedly, legitimate functions. There has been contentious debate on the legitimacy of guns and whether they should be banned, particularly in countries such as the US that dominates dialogue on gun control regulation. Legal approaches such as regulation have also been enacted in jurisdictions in order to allow but "control" certain activities. For example, the requirement for gun ownership in Germany is a psychiatric test and a minimum age requirement.[138] Strict systems of rules by such social institutions have also been applied to instrumental technologies, seemingly practical and useful devices that have the probability to be used for illegitimate use. In Japan for example, lock picking tools are strictly banned[139] while this may not be the case in other countries.

Criminalisation has been used as an approach to prevent events that antecede crime. Chatziioannou (n.d.) makes the argument that banning "hacking tools" may be a realistic approach to prevent events that presage acts related to the attack of computer systems, and specifically refers to underground forums where such tools are circulated. Criminalising software has also occurred as a means to protect copyright in the US. Software is evidently banned as implied in the *Digital Millennium Copyright Act* (DMCA), which effectively forbids any such tools, including software, that attempt to circumvent access-control measures that are designed to protect copyright.[140] The use of criminalisation to control these acts has raised considerable debate as to its legitimacy. When encryption technology was in its infancy in the 1990s, Phil Zimmerman, a security consultant in the US, was investigated for breaching the *Arms Export Control Act* for distributing a program he wrote that allowed others to encrypt their files and messages (Sussman, n.d.). With the importance of cryptography in World War 2 and its role in state security, technologies

[138] *Federal Weapons Act* (German: Waffengesetz), 1972.
[139] Japanese law on the prohibition of the possession of special lock picking tools. Source: http://law.e-gov.go.jp/htmldata/H15/H15HO065.html (source is in Japanese)
[140] The legitimacy of the US *DMCA* is highly contentious topic. For further details, refer to the Electronic Frontier Foundation (EFF) at https://www.eff.org/issues/dmca

associated with early developments of cryptography in the US were once restricted from being "exported" to other countries.[141]

Table 7 highlights countries that have criminalised software tools for the purposes of cybercrime with express substantive provisions. The first countries to ban such tools include the UK and Germany, followed by China and Japan (Broadhurst & Chang, 2013, p. 55). Common to the jurisdictions listed is the prohibition of the *transfer* of such software. In the case of Germany and Ukraine, the *creation* of the software is also proscribed. In the US, a *mens rea* requisite is included, that is, it is only illegal if an individual "knowingly" performs the cybercrime act.[142] For the case of the US, it is the act of *transmission* of software that is outlawed.

[141] Rules for export of cryptographic technologies in the US have become more lax since the 1990s.
[142] In the 2013 UNODC report on cybercrime, a reference is made to "computer misuse tools" which also lists relevant regional and international instruments, however, "tools" is loosely used to refer to any device, which also includes computers, used in the crime commission process and does not explicitly refer to software or programs.

Table 7: Countries that have criminalised software tools used for cybercrime

Country	Legislation	Partial extract
United Kingdom	Section 3A, Computer Misuse Act 1990	"A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under ... A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence …In this section "article" includes any program or data held in electronic form."[143]
Germany	Clause 202c	Translated: "… Producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible … software for the purpose of the commission of such an offence"[144]
China	Criminal Code 7th amendment in 2009 – Article 285 para. 2 and 3	Translated: "… Whoever provides special programs or tools for accessing or controlling a computer, or knows that the person committing the act will use the special programs for such purposes and provides the special programs, if the circumstances involve breaking the law, will be punished."[145]
Japan	Article 168-2 Criminal Code	Translated: "The amendment adds three areas subject to punishment: 1. to create or provide (a) electromagnetic records of a computer virus or (b) electromagnetic records and other records describing the computer virus (records of source code that may not function as a virus by itself but which is executable as a virus after translation into machine code), in order to put them into for use on a computer of another person ... 2. to put or attempt to put (a) into for use on a computer of another person ..., and 3. to obtain or store (a) or (b) ... "To put" them "into for use on a computer of another person" means making it possible that another person would (unknowingly) execute them on a computer."[146]
Ukraine	Article 361-1 Criminal Code	"Creation for the purpose of use, dissemination and distribution, as well as dissemination and distribution of harmful software or hardware, appropriate for unauthorized interference with the work of electronic computing machines (computers), automated systems, computer networks or telecommunication networks ... shall be punishable ... The same actions, if repeated or committed by a group of persons upon their prior conspiracy, if they caused a significant damage ... shall be punishable ..."[147]
United States	Computer Fraud and Abuse Act 1986	"[Whoever] … knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; …"

[143] *Computer Misuse Act* 1990, Section 3A can be accessed at http://www.legislation.gov.uk/ukpga/1990/18/section/3A

[144] Translated from German by Prof. Dr. Michael Bohlander at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1754

[145] Translated in 2013 from Chinese to English by Sergeant Da Chen, Cybercrime Division, Ministry of Public Security (China)

[146] Translated by Assoc. Prof. Kazutoshi Sugimoto at http://www.waseda.jp/hiken/en/jalaw_inf/topics2011/005sugimoto.html

[147] Translated version can be found on the UNODC SHERLOC database at http://www.unodc.org/cld/en/legislation/ukr/criminal_code_of_the_republic_of_ukraine/special_part_-_chapter_xvi_/article_361-1/article_361-1.html?

To date, the *Convention on Cybercrime* (hereinafter referred to as the Convention), released by the Council of Europe in 2001, is the first, and only, international treaty that seeks to harmonise laws and regulations of different national jurisdictions to tackle the problem of cybercrime. With only 47 countries that have ratified the treaty, which include eight non-European countries, there continues to be a large number of countries that have yet to accede to the Convention. Russia and China, who have not acceded to the Convention, have discussed a "UN" treaty on cybercrime (Brenner, 2014; Broadhurst & Chang, 2013). With some countries preferring to adopt the Convention as an international treaty on cybercrime, countries like Russia and China have pushed for a new agreement.[148]

In Article 6 of the Convention, it prohibits "the production, sale, procurement for use, import, distribution or otherwise making available of ... a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences ..."[149] From the explanatory notes, it is stated that the impetus of this prohibition is to prohibit such "hacker tools" as it is often used in the crime commission process and made available in underground markets. More recently, the EU has taken steps to criminalise certain software used in cybercrime. In Article 7 (Tools used for committing offences) in *EU Directive 2013/40/EU*, there are provisions that criminalise:

> … the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences … a computer programme, designed or adapted primarily for the purpose of committing any of the offences.

The provision also criminalises data such as "a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed." The EU has included the requirement of "intention", however further clarity is needed to interpret the term "without right". The point of contention by the opponents of

[148] Cybercrime scholars have debated the importance of a UN treaty on cybercrime. Judge Stein Schjolberg is one such scholar that has proposed a draft of a UN treaty on cybercrime. Relevant publications can be found on his website at: www.cybercrimelaw.net

[149] Article 6, Misuse of devices, *Convention on Cybercrime*, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

criminalisation has been that international, regional and national laws may be interpreted as a form of strict liability in which the mens rea element is not considered. Mere possession of crimeware would be illegal in such circumstances.

Article 2: "Hacking tools" banned in the UK

In 2008, legislation came into force in the UK that made it illegal to create and distribute "hacking tools". The measure was considered controversial at the time, largely from the security industry, due to the lack of clarity on what constituted such tools. According to a blog post by Andersen (2007), from the University of Cambridge Security Research Group, the legislation remained ambiguous despite the *Crown Prosecution Service guidance* publication that was released which is taken into account before a prosecution, which aims to clarify uncertainties.

Amendments were made to Section 3A of the Computer Misuse Act in the UK through the Serious Crime Act of 2015, which made it an offence "regardless of an intention to supply" certain software used for cybercrime. A mens rea element was highlighted in the explanatory notes that states, "the accused, at the time of committing the act, … [must know] that it is unauthorised" to show criminal intent.

The territorial scope of Section 3A was also expanded to make it an offence even if the person committing the offence was outside the UK.

It should also be noted that Section 57 of the Terrorism Act of 2000 in the UK also makes it an offence if an individual "possesses an article" and if that "possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism". It is ambiguous what an "article" may constitute.

Article 2. *Serious Crime Act* 2015. Retrieved from http://www.legislation.gov.uk/ukpga/2015/9/section/42/enacted
Commentary on Sections. Serious Crime Act 2015. Retrieved from http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/1 and http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/2
Terrorism Act 2000. Retrieved from http://www.legislation.gov.uk/ukpga/2000/11/part/VI/crossheading/terrorist-offences

The interpretation of what constitutes software that would be unlawful was evident among the web forum site members. The following section reveals how law is perceived from the perspective of the web forum site members. The underlying theme in the examples shows that there is inconsistency on the perceived legality of certain activities and types of crimeware. The view of law and criminalisation from the interviews with crime responders will also be presented.

It is evident that individuals had different views whether the activities they were involved in were moral. In the following example, the [OP] states they have infected over 500 victims with a remote access trojan called *DarkComet* and is unsure what to do next. [R7] responds to the [OP] to remove the remote access trojan targeted on a victim's computers as it was illegal.

> [OP]: Hi Guy, I have in my DC RAT [DarkComet RAT tool] more than 500 victims but what to do with them?
> [R7]: Make Internet Explorer their default browser and then uninstall them because what you're doing is illegal.
> (Forum C2 Thread #28)

Whether certain crimeware tools were in fact illegal such as remote access trojans were argued by certain members. In the following example, the [OP] states that the key differentiator between a legal and illegal remote access trojan is whether the user of the computer of which the remote access trojan (RAT) has targeted has been notified of its presence.

> [Topic]: Newbies Beginner Guide for RATs
> [OP]: In this thread I give you a few pointers to what a RAT is. ... Are RATs legal/illegal? Well, It is actually both. There are RATs that are legal and that are actually illegal. The difference between them both are the fact that, legal RATS inform the connected remote that you are on the computer, and illegal RATs do NOT inform the remote that you are on the computer. So basically to break things down. Legal means the person [owner of the computer] has full control as well, they can kill the connection [shutoff access] any time they please … illegal means the person [owner of the computer] does NOT know you are connected and they have no knowledge you are [there] till you take action. They have no control to kill the connection, unless they unplug the Internet, but even then, a backdoor is left on the computer meaning anytime the computer is on and the Internet is up, you can connect anytime you want. You can destroy files, download files, steal information, and basically make their life miserable.
> (Forum E8 Thread #30)

Similarly, the following [OP] states that a "legal" RAT is one that does not connect surreptitiously to a computer and is able to be shut down by the owner of the remotely accessed computer.

> [Topic]: Remote Administrator Tools Q&A?
> [OP]: ... Question - Legal or illegal? Answer - Well some RATs are legal, and some are not. Legal are the one without backdoor left, and they have ability to close connection anytime. Illegal are used for hacking and they can steal data like credit cards, passwords, private data etc …
> (Forum E8 Thread #36)

The legality of a remote access trojan depends on the intention of its creator. The [OP] in the following example mentions that another remote access trojan, known as *CyberGate*, is legal and implies that it is legitimate as the original author allegedly designed it for legitimate use. The [OP] also alludes the point that the user's intention should determine legality. Interestingly, the [OP] justifies the case of using a remote access trojan if used for reasons to guard children from harm.

> [OP]: Question: Is CyberGate illegal? Answer: No. CyberGate is a legal RAT. The author of CyberGate created his program for legitimate purposes. For example, there are many legal activities. Parents can use keyloggers to protect their children from online abuse etc. Some people use it for stealing passwords, credit cards and more but it's not a software, which breaks the law, but the person who uses it [or the intention that determines whether it is illegal].
> (Forum E7 Thread #23)

According to another member, crimeware tools should not be considered strictly illegal if used on their own computers for personal use. Although the [OP] in the following thread states their end goal for using a remote access trojan is for malicious purposes, they raise an interesting point of whether using a crimeware tool on one's own computer, or networked environment, should be considered wrong.

> [OP]: Ok, so I've got some pretty solid newbie questions I suppose. I never tried RATing anyone [using a RAT to illicitly access another person's computer without their knowledge], but … would like to try this someday. Firstly, I want to test some programs, form grabbers [keylogger] seem like the way to go for me. So I want to install SpyEye/ICE 9 [two relatively prevalent keyloggers among the web forum sites] from files distributed on this board on local host [target their own computer] … yes, my network, I know … Is it still illegal if I am using applications that are designed for illegal purposes on "legal terms"? … I want to RAT my own computers

and test if the grabbers are configured properly and if they work and are sending necessary info to my database …
(Forum D3 Thread #8)

Similar to the previous example, the legality of certain crimeware is discussed in the following thread. The [OP] raises the question of whether simply having a program for the purposes of learning would be criminal and if the program has to be used specifically for crime to be considered illegal. Interestingly, the response by [R1] and [R4] reveal that legality is dependent on the jurisdiction. [R1] also states that Europe has more strict laws. [R2] raises an interesting point on the vagueness of definitions. [R3] suggests that there is *a degree of criminality* with some tools that may be considered more harmful than others.

[Topic]: Question regarding programs.
[OP]: Hello. First of all, I would like to say that I am new to this site, and I am new to hacking. Before you redirect me to the FAQ [separate area on the web forum site where frequently asked questions are posted and answered], I already know about it and find it very helpful. One thing the FAQ doesn't cover, that I am very curious about, is programs and their legality. I know that almost all hacking programs are illegal to use … My main question being, is owning the programs illegal? Say I download the programs for learning purposes, are they illegal to have on my computer, or just illegal to use? I don't want to be lifted off to court for owning programs for the pure purpose of learning. Thank you for your answers.
[R1]: Depends on the country. Europe tends to have more strict laws, making the ownership of programs designed for malicious use illegal.
[R2]: But how do they define "programs"? And how do they define "ownership"? That laws are just stupid!
[R3]: … if its just for learning and you're using them in a VM [virtual environment setup on the computer of the user of the tool] and not out in the open [for example, used to compromise other's computers without their knowledge] you should be fine. It also depends on what programs you are using. Courts are going to look down on owning a compiled copy of Zeus [keylogger] more then they are a copy of nmap [network scanning tool].
[R4]: Technically they are only illegal, in the US, if you are using them maliciously. Like said above, using them for learning purposes are fine, as well as using them on your own network, or one that you have been authorized to use it on, but if you get in some sort of trouble involving your computer, and they search it and find it on there, it wont look very good for you.
(Forum D1 Thread #15)

Criminalisation may generate undesirable effects as described in an interview with an individual from a governmental response agency. It was suggested that criminalising certain tools, such as *nmap*, would not be feasible, as it would adversely affect legitimate professionals.

> You can't criminalise nmap [network scanning tool] and stuff [other security tools designed for legitimate use]. No one would be able to [do legitimate] work, it just won't work because these are things people use all the time. (Public sector #2)

As a solution to avoid strict liability, licensing was suggested as a strategy in which only certain individuals would be allowed to use crimeware programs, as mentioned by one independent security professional.

> Criminalisation is a complicated topic. It's really hard to show intent so I guess criminalisation does make sense. I'm wondering if licensing is an idea … certain tools can be regulated maybe. (Independent #1)

There may be a varying degree of maliciousness among the various crimeware that may be related to specifically designed criminogenic features. The [OP] in the following example suggests that bots of a certain type are "more" illegal than others. The [OP] states that bots associated with "banking" trojan activities are clearly wrong, as it has the function to steal banking and financial related details of a victim, which is sent to the cybercriminal.

> [Topic]: Tutorial - Setup Zeus Bot with Pictures & Tutorial
> [OP]: This Tutorial is for education purposes only and I am not responsible in any way on how you use the information provided and what you do with the files. Thank you and enjoy reading. First of all I want to tell you that ZeuS Bot is the most illegal bot out there. It is the only bot that connects to a webhost and not to an IRC channel [botnets communicate via website servers, not chatrooms] or a PC. It is highly illegal as it is considered as a banking trojan [contains code specifically to target banking related data such as login credentials] as it logs every Internet activity to a database. Well let's start …
> (Forum E6 Thread #72)

Relationships between law and society are present which concern web forum site members, institutions such as law enforcement, the private industry that develops technologies and

services to protect from cybercrime activities and the law. The German sociologist Niklas Luhmann, a major proponent of using systems theory[150] to explain law, has pointed out that this relationship between law and society is inadequate and requires more judicious inquiry (Luhmann, Ziegert & Kastner, 2004). Criminalisation has been used in society to address crime, however there are limits and consequences to such an approach particularly when it has the potential to stifle the industry that has legitimate utility.

6.2 Benefits

Online criminal activity feeds the cybersecurity industry. As Shelden, Brown, Miller and Fritzler (2015) pointed out on the topic of the crime control industry, private security is one of the fastest growing areas of the *criminal justice industrial complex*. Referring to businesses that profit from crime, the observation by Shelden et al. (2015) also has relevance to the Internet security industry with annual revenue in the billions. Andersen et al. (2013, p. 350) approximated that the global purchase of antivirus products amounted to $3.4 billion in 2013 with corporate spending on botnet protection products and services to be around $10 billion. From botnet-specific detection services to network firewall equipment designed to block unwanted Internet packets, it is patent that an assortment of products and services are available in the market geared toward ensuring online safety and security. According to Choo (2007), it is the different companies in the private sector that are best situated to help reduce risk for Internet users. It is undeniable that the private sector has driven the advancement of Internet security technologies with products developed and made available to home users, as well as to the larger organisation and enterprise. The

[150] The focus of *systems theory* involves investigating the abstract relationships, dependencies and interconnections of various phenomena with applications in different bodies of knowledge from the environment to science. Originally proposed by biologist Bertalanffy (1968) in the 1930s, system theory has its roots mainly in biological processes and systems. Also originating from the biological focus is Millers (1965) living systems theory, which views living systems as "self-organizing" and constantly connected to the environment. Buckley (1967) was the first to introduce concepts of systems theory to the field of sociology, however it was functionalists Parsons (1951) and Luhman (1975) that appropriated and developed systems theory in sociology, which explains that an individual cannot be understood in isolation but as a part of a larger group. Systems theory has been relegated along with the decline of functionalism, although there have been some minor developments in sociology (Bailey, 1994) and has later manifested in *complexity theory* (Bailey, 2001). Systems theory will not be explored in depth in this thesis, although some of its principles are used. The key point to take from systems theory is that society consists of many different groups that are interconnected.

private Internet security industry is expansive and has continually developed new ways to protect users from cybercrime, but also faces challenges. For example, stopping malware by matching its "digital fingerprint" is declining in its effectiveness to harden targets (Li & Clark, 2013).[151]

An interdependent relationship exists between the actors that engage in cybercrime and the cyber-*criminal justice industrial complex*. Kshteri (2010) highlighted the cybersecurity industry to involve economic and institutional processes. It is palpable that cybercrime activity perpetrated by offenders has affected the growth of the cybersecurity industry. The creation of new forms of crimeware by malicious actors is typically followed by a response from the "industry" through the development of new technologies to mitigate the undesirable activity. The public distribution of crimeware in web forum sites has further exacerbated this issue, with the number of offenders able to gain access to crimeware "tool kits" and botnets multiplied (Yar, 2005; Wall, 2007). It is this recurring and ongoing progression of online threats that has increased risk for Internet users.

Both the private and public sector have responded to incidents of cybercrime, by creating new jobs and professions. Internet security professionals particularly in the private sector have benefited from job opportunities due to cybercrime, as stated by one respondent.

> I know of a lot of people that have made careers in this [IT security] field, including myself … here [in the local city] there are a lot of big corporations that have set up shop the past few years. It's fun work. I know one big company that does some great malware investigation work just next door … they are hiring now. (Private sector #3)

Furthermore, there was indication that people were visiting the web forum sites for the purpose of developing their careers. Individuals visited the web forum sites to solicit guidance on skills required to pursue a career path in malware analysis. In one such case, the [OP] asks which programming languages would be useful to know in the future for malware analysis. The subsequent responses recommend different programming languages

[151] The term "digital fingerprint" is used to refer to signature-based approaches to detecting malicious forms of software.

such as C, C++ and C#, which are debated among the members. The discussion is shown below.

> [OP]: I have learned the basics of Java but that is all. I want to be useful in the future though so I am asking which language I should specialize in. Which do you envision being a major language in 2 or 4 years from now? This is in the sense of malware and analysis. I wish to have a long tech career and I'm looking for any advice on malware code and asking for help deciding my near future and what language I'll be dedicating countless hours to in the years to come.
> [R1]: … you need to know one of the system programming languages, so in my opinion C# is a very easy language in system programming, my suggestion for you is to start learning C#.
> [R2]: Dude, are you fucking trolling? Suggesting a .NET language for Malware? C is the best language for advanced Malware … why do all of the new most successful Malware programs use it?
> [R3]: … I don't actually like .NET Languages, so I think you should learn C/C++
> (Forum A2 Thread #35)

Such communities also function as sources of information on malicious techniques. In one case, one member inquires about website defacing techniques and states their reason to obtain such knowledge is to embark on a career path in cyber warfare. In the following example, the [OP] states that they would not be defacing any websites and implies the inquiry is legitimate.

> [OP]: First off, I'm not going to use this to deface websites, just want some info. I understand how to compromise sites, but how do you go from getting information to changing the page? Is it as easy as finding the admin account and going from there, or is there a better way? …
> [R1]: There's really no skill involved with defacing. There's a lot of different ways …
> [R2-OP]: Okay, thanks for the fast reply. Yeah, it is a waste of time, but it just seemed kinda interesting, and since it is one of the most common forms of hacking. I'm looking at a career in cyber warfare, just seemed logical to know some of the basic steps.
> (Forum B1 Thread #34)

The significance of the previous discussions is that crimeware communities do offer some level of benefit to Internet security professionals and cybercrime responders as they provide insight into the techniques of cybercrime and offers a source to learn skills required for

technical investigations. The skill set between legitimate Internet security professionals and cybercrime offenders are conceivably similar. As shown in the examples, members can have honest and legitimate motives. Individuals with benign goals, as revealed previously, visit the same web forum sites as individuals with malicious intentions.

The problem of cybercrime, and crimeware activities, has also impacted the public sector encouraging responders to learn new skills. In certain cases, new professions have developed to fulfil the needs to respond to cybercrime. For example, one governmental cybercrime response agency provided financial support for computer-related education to its employees.

> Got about 20 people now in our team that look at cybercrime cases, which is not enough. There are so many cases requiring very specific skills … it's pretty much just picking and choosing which we want to look at, but we need to be able to handle the investigations properly. One of the problems is that we don't have enough skilled staff. This is why we encourage education …we have one person studying computer science part-time at university and another doing their Certified Ethical Hacker certification … we subsidise some of their schooling. (Public sector #1)

Article 3: Growth of the cybersecurity industry

According to CB Insights, venture capital and private equity based funding for cyber security start-ups have shown a general increasing trend in terms of total funding. The increased reporting of cyber attacks has influenced seed-stage investments, which generally involve investment in smaller businesses at a very early stage until it can generate revenue on its own. The top locations for cyber security start-ups include Silicon Valley, Israel, Canada and the UK. The growth of the Internet security is a common trend in many countries with new companies generating new jobs and the requirement of specific skill sets.

Article 3. *As Threats Increase, Cybersecurity Software and Hardware Sees Uptick in VC Deals and Funding – $1.4 Billion Across 239 Deals in Last Year*. Retrieved from https://www.cbinsights.com/blog/cybesecurity-venture-capital/ (CB Insights, 2013)

The underlying principle of Bentham's (1891) expression of the "greatest-happiness principle" holds that the greatest collective happiness of the population takes precedence. The "utility", specifically its presence and use by actors, of crimeware in society presents a contradictory view. Contradictory to the effects of crime, the web forum site as a setting for crimeware discussions may be seen as offering a conceivably constructive value for

society. It is important to clarify that it is not being stated that *crime is good* but its by-products may be connected to certain institutions and practises. Perhaps this could be viewed as a consequence of an *unintended consequence*, that is cybercrime is an unexpected result of the emergence of the Internet and at the same time the potentially useful effects to society is an unexpected result of cybercrime. Interactions with offenders, access to crimeware tools and relevant knowledge on web forum sites generates information that indirectly helps to secure systems.

On the web forum sites, certain members inquired about how to protect their computer systems. Not all discussions related to activities of a harmful or damaging nature. For example, one member asks a question on how to check whether a keylogger was installed on their system that may be covertly capturing their keystrokes. The replier [R1] directs the [OP] to download a software tool, which provides such a feature. The replier [R1] also mentions to make sure the tool is "clean" and recommends scanning it through a free malware detection service known as *VirusTotal*.[152]

> [OP]: How do I make sure there isn't a keylogger on my computer?
> [R1]: Use hijackthis [software] to see what is running and installed, you can use virustotal.com for file scanning [to check if the keylogger is backdoored].
> (Forum D1 Thread #8)

Turgeman-Goldschmidt (2008) suggested that Internet security professionals benefit from the knowledge of hackers. The previous example shows one example that web forum sites provide information on how to remove malware, which discernibly does not cause any sort of damage or disruption to a computer. It was also common for web forum site members to inquire about methods to protect their computers. The [OP] in the following example reveals that someone on the web forum site may have hacked into their computer and asks for advice on how to secure their laptop.

[152] *VirusTotal* is a free online service that checks for malicious files that aim to infect users. The service is located at www.virustotal.com. It should be noted that VirusTotal employs a signature-based detection approach to detect malware, which has been reported in the computer security industry to being increasingly ineffective. Contradictorily, VirusTotal is used as a resource to help identify and protect systems from malware but is also being used by individuals who use malware to target victims.

> [OP]: How can I secure my laptop? Ever since I started coming on here someone has been getting into my laptop [accessing the computer]. Once I notice it happening, I reboot immediately and do a scan with Norton and Malwarebytes [two anti-malware products]. What else can I do? Someone keeps on changing my password. It's getting annoying.
> (Forum H1 Thread #13)

As mentioned in Chapter 3, one of the web forum sites selected earlier in the study, known as *VX Heavens*,[153] was removed from the study as it was taken down by law enforcement during the data collection process. The following message was posted on the *VX Heavens* website when it was shut down:

> For many years we tried hard to establish a reliable work of the site, which supplied you with a professional quality information on systems security and computer virology … [on] Friday, 23 March, the server has being seized by the police forces due to the criminal investigation … (Maurushat, 2013, p. 27)

According to Maurushat (2013) the *VX Heavens* site was a malware community frequented by individuals with benign intentions and was not known to have links to organised crime. Maurushat (2013) speculated that the site was taken down due to political reasons. If Maurushat's conjecture is accurate, the take down of sites such as *VX Heavens* may have unintentionally affected individuals with legitimate non-malicious reasons that had visited the site. Such individuals are likely to include security researchers and professionals seeking information for legitimate purposes.

Incidents of cybercrime have also prompted organisations and Internet users to protect themselves from online threats. Without incidents of malicious online activities, there would be little incentive and effort to ensure systems and devices are sufficiently protected. In one interview, the respondent implies that the increasing risk of cybercrime activity was the main reason they were hired.

[153] The name *VX Heavens*, short for *Virus eXchange Heavens*, has not been redacted in study as it was not formally included in the data collection. *VX Heavens* was a malware web forum site hosted in Ukraine. The site was shut down by Ukrainian law enforcement in early 2012. Only a small amount of data was collected from *VX Heavens*, insufficient for analysis, and for this reason was removed from the study.

> We have people from government going to the private sector, and people working in the fraud department of banks going to other banks. There is a lot of movement … cybercrime is a growing problem everywhere. With all this hacking happening, big companies have been throwing around money to pay people like me to make sure we keep up with best practices … we make sure systems are properly setup to stop hackers. This is even more important now … there have been a lot of hacking intrusions over the past year. (Private sector #3)

It has also been suggested encountering consistent and manageable incidents of cybercrime has been, at some level, advantageous. Elazari (2014) also makes this observation when alluding to the Internet mirroring the immune system and cybercrime being its virus. Simply put, viruses ultimately strengthen the immune system. For example, investigating smaller cases of online fraud more frequently has been useful when investigating larger fraud cases.

> Without the constant barrage of online fraud … no one would get off their ass and do anything. Seeing fraud every week has been helpful because we learn from them. Not saying [online fraud] crime is a good thing, just saying seeing it keeps us on our toes until something big comes along. We learn from the small ones. (Private sector #2)

Article 4: Metasploit used by law enforcement

Metasploit is a computer security tool that reveals details on vulnerabilities on a system. It is a security tool designed for use by information security professionals. The tool is often purported to be used by cybercriminals.

In a 2012 online sting operation, the FBI obtained permission by a federal court to infect visitors of a Tor website under investigation. Tor is an Internet technology that provides anonymity to websites and its visitors by encrypting the IP address path between the source and destination, making traffic untraceable. By infecting the visitors with malware, tailored by the FBI, the IP address of visitors could be revealed and visitor location's identified. The malware designed by the FBI relied on a Metasploit add-on feature known as the Metasploit Decloaking Engine.

Article 4. *FBI Used Metasploit Hacking Tool in 'Operation Torpedo'*. Retrieved from http://www.tripwire.com/state-of-security/latest-security-news/fbi-used-metasploit-hacking-tool-in-operation-torpedo/ (Bisson, 2014)

6.3 Social Uncertainty

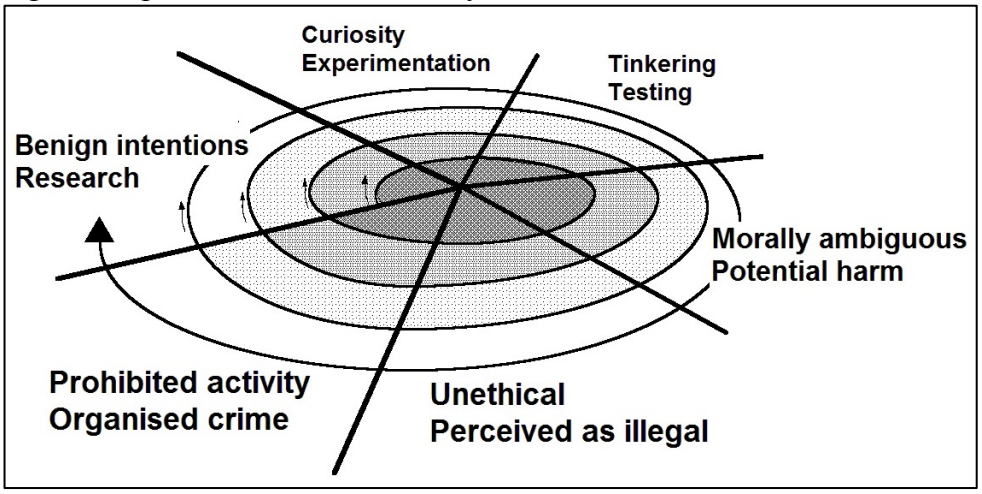
The rejection of norms can lead to uncertainty and instability in society. Merton's (1938) view of normlessness, which was referred to as anomie in his strain theory, referred to the circumstance when the goals to achieve success in society did not provide for legitimate ways to achieve such goals (it is anomie that leads to crime, and the weakening of societal norms which Merton refers to as "anomie"). In contrast, Durkheim (1933) believed when social change occurred too rapidly, a collapse of norms happened which subsequently lead to a state of anomie. The equivocal nature of the creation of crimeware, expressed as the ambiguity between what is legal and illegal, is another theme that arose within the web forum sites and a possible illustration of Durkheim's view of anomie (the crime-like activities taking place due to an absence of norms, and values, and a lack of moral guidance describe the creation and distribution of crimeware). Additionally, the case of crimeware web forum sites that are publicly accessible is an indication of anomie with the imbalance of societal norms as the reason web forum sites involved in crimeware activities have formed. With this lack of norms, social uncertainty has developed, and it is society that is responsible for generating deviant and criminal web forum sites.

Criminal behaviour is often seen, imprecisely, as a dichotomy rather than as a continuum (as cited in Moyer, 2001, p. 74). Furnell (2010) suggested that the terms "black hat", "grey hat" and "white hat" have been used as labels for hackers to signal intent. It is apparent that members in the web forum sites in certain cases did not perceive particular actions as clearly wrong or as "black hat" rather as "grey". Likewise, Jordan and Taylor (1998) portray this transient nature of the hacker from earlier communities who can fall somewhere between the extremes of the career criminal type to the dabbler of cybercrime with skills that can degrade with time if inactive for too long. There appears to be moral ambiguity amongst members based on the observed interactions in the web forum sites. There is indication that members understood that certain activities were morally wrong, but the extent to which an action was perceived to be wrong varied.

Based on the web forum site interactions, the activities associated with crimeware are represented visually as a spiral (see Figure 6), which emphasises the circulating nature of crimeware. The same *piece* of crimeware is often created, distributed, used, explored, investigated or its activities stopped by various agents. Each quadrant represents the

different types of actors and their motivations who participate in the web forum sites. The spiral represents the tools, skills, knowledge, techniques and collaborators that circulate and flow amongst the different actors.

Figure 6: Spiral of crimeware activity



Not all activities were clearly delineated as either legitimate or unlawful by web forum site members. The following example reveals a discussion thread amongst two members who discuss ways to monetise remote access trojans. The key point of interest is the response from the replier [R6] who implies that the use of such crimeware for certain purposes may not be overtly wrong when collecting "behavioural" details of victims. The replier [R6] refers to such a technique as "grey hat", signifying that it is not clearly illegal.[154]

> [OP]: I have been weighing out whether to use a RAT or not, and the one thing that keeps coming back is how to monetize it [make money]. I thought about maybe putting adware on [make money by playing advertisements on compromised computers], but I want to be stealthy. I thought about maybe doing pins [to access peoples financial details such as credit card numbers], but after a few individuals explained the processes involved, I don't think it would be worth it. I also thought about maybe cookie stuffing [illicit access of a legitimate site which is used to spread malicious code to visiting computers], but how would you do that? I also thought maybe I could threaten to overclock their PC, and maybe overclock their PC if they did not give me money [taking control of a computer as a form of ransom]. I also

[154] This can also be viewed as neutralising behaviour. The web forum site member justifies their action that no one is victimised if the purpose is simply to "spy" on their targets.

> thought that chances are, at least a few of them have a PayPal account [with the goal to steal login credentials], and perhaps I could leverage that. Any ideas?
> [R6:] Lately, I'm thinking about using RATs too. One of the idea is data gathering victims interests, hobbies, products he wants etc. It's grey hat style but I think it's possible to make decent money without being arrested …
> (Forum D3 Thread #25).

Members with different motivations co-exist on the site. In the following example, the [OP] asks the question how they can progress to becoming a black hat or grey hat hacker. [R6] reveals in their response that they are a "grey hat" hacker and that they do not denounce malicious, potentially criminal, activities associated with black hats.

> [OP]: Hey, I'm a script kiddy and I want to be a black hat/grey hat hacker and just don't know where to go after being a script kiddy. All I can do is get IP's, DDoS lightly and yeah, it's not as fun as exploits.
> [R6]: It really depends, I suggest HTML first, and then C++ or VB.net or Perl [various programming languages]. HTML is a must - everyone should have a moderate understanding of it. C++, VB and Perl are all quite basic, but the reason you would learn one, is to learn 'how to learn' a coding language. From there, you can pick a new code, depending what you wish to do. Also, I don't frown upon blackhat activities. I am grey, so yeah.
> (Forum H1 Thread #7)

To point out an interesting observation, those with legitimate motivations also frequent such web forum sites. The varied composition of intentions, underlying motivations and associated labels by members reveals that such sites include a mixture of different types of individuals that interact with each other. Soudijn and Zegers (2012) suggested that carding forums provided a virtual location for *offender* convergence. However, the interactions on the crimeware web forum sites in the study identified a range of individuals with different goals, which ranged from legitimate, to possibly malicious and to overtly criminal intentions. The web forum sites were a convergence setting for anyone with a stake in crimeware, including non-offenders.

Labeling all web forum site members as cybercriminals remains dubious with individuals with different motivations participating on the web forum sites. When describing youth delinquents, Matza (1964) argued that youths drifted into delinquent and sometimes

criminal behaviour (for example, youths stray from the values of mainstream society and drift back when mainstream values become more important as they get older). The weakening of social ties with society was believed to be one cause of delinquency, according to Matza. With the increasing of social ties with society, the converse of Matza's argument could explain why certain "criminals" subsequently become legitimate law-abiding individuals. As raised in one of the interviews, certain individuals that were once black hats, over time took on a role working to help counteract cybercrime activity.

> I know some people doing both legit and illegit stuff … some of the co-founders at the company I used to work at were actually blackhats back in the day. When the rouble fell [in Russia], a lot of people turned to malware development as a way to make ends meet because they were out of work ... these were normal people like you and me, not criminals doing this stuff. These days governments are paying these same guys to work for them ... I was offered a job but I didn't like the conditions so I didn't take it. At the company I worked for just before [in the US], we hired blackhat consultants to teach us how to hack websites. (Independent #4)

Furthermore, there is indication that the composition of true offenders, potential offenders and non-offenders vary depending on certain factors such as the content of the web forum site, the targeted "audience", and hosting location of the web forum site server. In the case of Forum D, the only Tor[155] web forum site selected in the study, discussions related to illicit activity such as the deployment of botnets and techniques of fraud were more common. While in the case of Forum A, the largest forum examined in the study, rules were posted on the site that governed acceptable behaviour. Interestingly, Forum A also required users to comply with the *Children's Online Privacy Protection Ac*t (COPPA):

> In order to register on these forums, we require you to verify your age to comply with COPPA. Please enter your date of birth below. If you are under the age of 13, parental permission must be obtained … (Forum A)

A comparative analysis of the web forum sites was beyond the scope of this research, however it should be noted that the nature of the discussion content did appear to vary between certain web forum sites. For example, the members in Forum D, the Tor site,

[155] *Tor*, or The Onion Router, is a network that allows for anonymous Internet access.

appeared to be more open in discussing past cybercrime experiences. This may be due to the fact that the site is hosted on Tor, providing an additional layer of anonymity to members. Despite such variations, crimeware was discussed, distributed for download or provided access on all the sites in the study.

Article 5: Student expelled for finding vulnerability

Hamed Al-Khabaz, a post-secondary student in Montreal was expelled for accessing the personal details of over 250,000 students. A vulnerability was identified by the student using a tool called Acunetix which scans a website for security holes. The security flaw was reported to the college after it was found. Mr. Al-Khabaz told the National Post, "I felt I had a moral duty to bring it to the attention of the college and help to fix it, which I did…"

It was alleged that the president of Skytech, the company that created the website, threatened Mr. Khabaz stating that he could face jail time and pressured the student to sign a non-disclosure agreement. The security flaw was eventually fixed. The president of Skytech subsequently revealed that the student used the Acunetix tool again to check if the website was fixed.

Article 5. *Student Expelled for Hacking After Investigating Security Hole*. Retrieved from http://www.wired.com/2013/01/student-expelled-exposing-flaw/ (Zetter, 2013)

Academic research has contextualised the hacker subculture as a form of youth delinquency. Yar (2013) suggested the participation of youth in hacking activities could be explained by subcultural views of crime. Likewise, cybercrime has also been expressed as a subculture consisting mainly of teenagers (Team Cymru, 2006). In one of the interviews, a comment is made that botnet activities may be common among high school students.

> I know that most people see malware activities as something that happens somewhere like Ukraine. Most of the activities happen right here where we live. There is at least one botnet herder in every high school. I know the people running in the younger crowd think it's cool to have botnets. It's like a game to them. (Public sector #3)

Crimeware communities are also redolent of an underground or "alternative" subculture. Cloward and Ohlin (2013) suggested that the path to crime falls under one of three typologies of subculture. Two of these of relevance are the *conflict subculture* (a culture that arises when individuals reject both legitimate and illegitimate means to achieve success) and *criminal subculture* (a culture where illegitimate opportunities are made available).

Revealed in greater detail in Chapter 5, crimeware communities offer illegitimate opportunities, such as the knowledge of how to use particular crimeware tools when building botnets and coordinated activities for instance the hacking of targeted websites. It also provides parallel legitimate opportunities, as alluded to in Chapter 6.2 with the creation of new opportunities for legitimate industry. It is the availability of illegitimate pathways in the web forum sites that provide the opportunity for individuals to engage in cybercrime activity. As covered in Chapter 4, this process of pursuing illegitimate pathways involves social processes indicative of learning through online interaction.

Furthermore, crimeware communities are also characteristic of a *conflict* subculture. The inability to achieve success through legitimate means and the incapability of engaging in online criminal activities, without the assistance of tools, supports the idea of the formation of the *disorganised* crimeware community. Such communities act as sources where crimeware tools are distributed and visited by the potential offender to acquire specific tools and knowledge in order to engage in malicious online activities. Drawing from Cloward and Ohlin's (1994) differential opportunity theory, the illegitimate opportunity structure, for example advanced hacking skills, is absent for the offender forming *alternative* illegitimate opportunity structures, which has manifested as the web forum sites examined in the study. This notion of a subculture is also supported by the existence of discussion groups targeted to beginners and novice members who have little technical knowledge, which were found on all web forum sites in the study. Members that lack experience plausibly visit such sites where instead of engaging in more serious cybercrime acts, congregate on the web forum sites. The web forum sites may indeed be conducive to "learning about crimeware" and perhaps instigate law-breaking behaviour, but the archetypal *criminal subculture*, as Sutherland (1956) depicts as an underworld of professional thieves, may not be the most accurate categorisation of the web forum sites.

6.4 Crimeware Communities in a Social System

Wider society can be viewed as comprising "smaller" interconnecting parts that are dependent on each other. Drawing from Durkheim's view of that society is emphasised

over individual actions, Parsons (1951) stressed the function of systems and that individuals fulfilled the needs to maintain the functioning of a particular social system. According to Parsons (1951), a social system could be viewed as interdependent parts and the social groups within society could be viewed as smaller subsystems that exist within larger society, which he referred to as action systems. When explaining Parsons' view, Adams and Sydie (2001, p. 350) stated that such systems have connected parts within it. Parsons believed that each system had certain needs required for its survival. A sub-system would be unable to function or cease to exist without others.

The relevance of such a view is that change observed in one society is likely to happen in the same way in a different society. For example, the issue of cybercrime, which has detrimental consequences particularly to its victims, in today's technologically advanced countries may eventually be faced in other countries that are in the process of embracing Internet and computing technologies. In this section, the social groups and institutions in society that are highlighted, include offenders, law and the criminal justice system, or the *cyber*-industrial complex, as alluded to in Chapter 6.2. This section calls attention to the interdependent relationship between offenders and other groups and institutions, and the conflict and uncertainty within such groups, in society that aim to prevent cybercrime. Ekblom (2001) expresses one aspect of this relationship as an arms race between criminals and crime preventers. This section is a segue to the crime prevention implications raised in the subsequent section, Chapter 6.5.

An important question should be raised whether private business of the Internet security industry is considered to be in a role to prevent cybercrime activities on the Internet. In one interview it was stated that the Internet security industry helped to prevent the spreading of malware and has "filled in the gap" for the public sector. The private sector does conceivably help to protect against cybercrime in a different manner compared with law enforcement and the law.

> We see so many [cybercrime] cases that we just pick and select what we want to look at [investigate]. It's sort of ad hoc. I think AV [anti-virus] companies are more suited to stopping malware. We do look at the technical aspects of crime but our approach is

> sort of old fashioned. We wait until a person becomes a victim first and then we investigate. (Public sector #1)

Noted in one interview is the discord, namely the lack of cooperation, between guardians and victims. Certain institutions did not fully cooperate with the public sector. For example, institutions such as banks that are often the target of crimeware were noted not to report cases of cybercrime.

> Banks are only interested in their own needs. If a specific piece of malware targets them, then they only focus on that. They don't care about anything else, and they never disclose anything bad that happens. It's just too risky to let that stuff [cases of cybercrime] get out to competing banks. That's why they don't report anything to the police, and when they do report something bad it's usually too late. (Private sector #2)

This tendency to avoid sharing information of cybercrime incidents is also related to the risk of revealing details on infrastructure, which creates risk if revealed, such as suggested in the following interview.

> I'm certain that other groups in the same industry as us also face the same issues and challenges when responding to online fraud, but we don't share data with them. Discussing this stuff [incidents of cyber attacks and fraud] can be risky because it exposes confidential details on our systems. (Independent #2)

The lack of sharing was also evident between the private and public sector as revealed in one interview.

> The private sector releases reports very quickly after some big event [a big cyber attack], which ultimately influences public knowledge. One problem is that the private sector doesn't share its investigative work with the public sector. (Public sector #4)

Parsons (1951) also believed that every social group in society fulfilled "functional imperatives", one aspect of it which included the ability of a social group to adapt to the larger social environment, in other words, society. One example of this is innovation that

was discussed in Chapter 5.2. Crimeware communities, as a social system, continue to subsist while the criminal technologies developed continue to improve and advance.

Additionally, Parsons (1951) conceptualised the connections between social groups and institutions as feedback loops or exchanges that lead to an equilibrium, along the traditions of functionalist views of society that was described earlier in this chapter. The relationship between crime preventers and criminals could be explained as an arms race (Ekblom, 1997; Ekblom 1999). This is clearly discernible as it was revealed in Chapter 5 that crimeware tools were innovated by web forum site members in order to circumvent institutions aimed at preventing crime. Grabosky (2001) suggested that crime prevention measures may in, certain cases, produce unintended consequences. It was suggested in one of the interviews, as shown below, that it was difficult to track cybercriminals as they continue to change and evolve. Crime preventers may unintentionally influence the behaviour of cybercriminals, in effect driving cybercriminals to change.

> Identifying crime and then talking about it publicly can cause criminals to change. This is counterproductive because you want to stop these people but if you make public the technical details of some crime, the bad guys change their MO. (Independent #5)

As suggested in Chapter 6.2, certain legitimate social groups, such as the Internet security industry benefit from cybercrime. As different groups within the system are mutually dependent, this relationship could be characterised as a feedback loop.[156] Crime preventers deploy technical measures to stop cybercrime, which ultimately influences offenders to change their behaviour, patterns and actions. From the viewpoint of Wortley's (1998) precipitators, it is the crime preventers that paradoxically prompt and provoke offenders. In one interview, it was implied that the constant modification of malware by cybercriminals was in part triggered by the measures developed by the private sector to stop them.

> Cybercriminals are always one step ahead of us, and we just can't catch up. Every time we release an update, it becomes ineffective very quickly. They [the criminals]

[156] This draws from complex adaptive systems. Refer to footnote 135 for a brief description of complex adaptive systems.

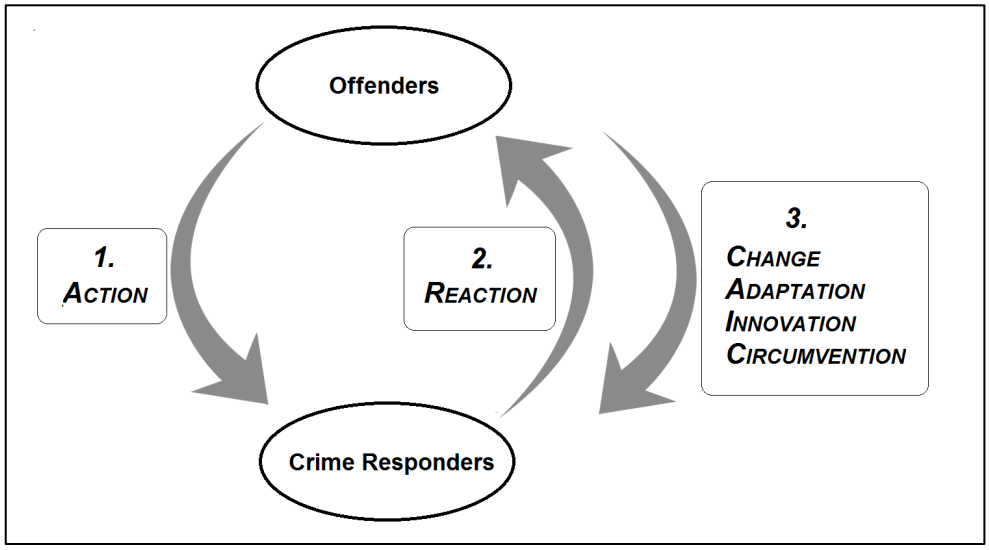
> are winning. Everything we do is rather manual. We find some malware and write a signature to block it. The problem is there is too much malware. It's constantly in flux. (Private sector #2)

The public reporting of cybercrime by the private sector may also serve to conceivably contribute to cybercrime. Wall (2008) suggested that the media that may be *fanning the flames* on cybercrime as a problem, in a manner creating "moral panic" (Cohen, 2002), thus shaping public perceptions. In one discussion with a private security professional, it was raised that the private sector may contradictorily be promoting cybercrime.

> I was at a conference once and there was a big presentation from one law enforcement agency. The guy said [in the presentation] people shouldn't be releasing details on investigation work [on cybercrime incidents] because it helps the criminals. I totally did not agree with this. Investigation work [from the private sector] is needed. I think what I do is very helpful. (Private sector #2)

A visual depiction of this feedback relationship between offenders and crime responders (crime preventers) is revealed in Figure 7. Offenders proactively make an effort to create crimeware and use techniques for the purposes of engaging in crime (denoted as 1.). Subsequently, crime responders, particular for the case of the private Internet security industry (as described in Chapter 6.2), develop technologies to guard against the actions of offenders (denoted as 2.). The feedback step occurs when offenders react or pre-empt the actions of cybercrime responders through techniques that essentially involve outwitting them (denoted as 3.).

Figure 7: The feedback relationship between offenders and crime responders



The "good versus bad" dichotomy of criminals and law enforcement may be one-dimensional. This antagonistic relationship may best be described as mutually dependent, as the relationship is one that is based on a continual cause and effect process.

6.5 Ramifications for Crime Prevention

There are certain implications for crime prevention strategies based on the data in this research. The following section raises general questions that have potential consequences on strategies that aim to reduce cases of cybercrime, namely the relative significance of the crime in question, the issue of ambiguity in law, the unintended outcomes due to certain crime prevention measures, and throughout the section, suggests potential approaches to prevent cybercrime based on the data.

The fundamental question is whether the development and distribution of crimeware and its associated activities should in fact be considered criminal. The conventional approach when determining the legitimacy of criminalisation has been to start with the harm principle. Mill (1869) proposed an important conception on the use of power that people's choices should only be restricted if the sole reason is to prevent harm. It is certainly evident that indirect harm of people is incurred in cases of hacking incidents and data theft, as well as larger organisations that are adversely affected. The *proof* of harm (the confirmation that harm has

taken place) in certain cases is overlooked (Green, 2009) potentially leading to *too much* criminalisation. As highlighted in Chapter 6.1, one approach to deter cybercrime activities has been to criminalise the potential precursors to crime, which has lead to the enactment of new laws.

Commonly raised rhetoric, particularly from the legitimate computer security sector, is attributable to the reason that the banning of "hacking tools" has been ambiguous. Legitimate security tools may fall within such a broad definition (see Article 5 in Chapter 6.3). This has been addressed with the incorporation of a mens rea element, in certain jurisdictions, although not explicitly clarified how this could be established, which is often raised. A possible case of strict liability, it would imply mere possession of crimeware tools would be enough to hold the owner of the computer containing such software liable. Another key problem with criminalisation is whether the defining rules are too limited in some situations or too broad (Golding & Edmundson, 2008, p. 112). A suggested approach in addressing this problem could be drawn from strategies in handling other criminal activities. For example, in the criminalisation of illegal drugs, one strategy involves the classification of different types of drugs, whereby the substances with more addictive or harmful properties are more strictly controlled or deemed illegal; perhaps such a controlled form of criminalisation could be applied to crimeware. Challenges may arise though as crimeware changes and evolves at a comparatively fast rate and so classifying such software is difficult when it evolves so rapidly. Rather than relying on *harder* forms of control such as prohibition, *softer* approaches through regulation is another possibility.

The efficacy of current responses to cybercrime is contentious. Responses to cybercrime could also be viewed as potentially iatrogenic. Cybercrime is assumed to be caused by crimeware; to address cybercrime, the approaches in certain jurisdictions has been perhaps *heavy-handed* by illegalising any software potentially used for cybercrime. Clarke (2012) offers the situational method as an alternative, however, the ways in which software can be restricted in practice is uncertain without legalistic approaches. The contention arises from the fact that certain crimeware tools are not intentionally created for cybercriminal purposes rather such tools have been manipulated for such use.

Additionally, the inefficacy of law on controlling cybercrime has also been attributed to the lack of relevant technical knowledge on the part of criminal justice practitioners. To address this, a suggestion is to improve the sharing of knowledge between the private and public spheres in Internet security. From the research, one interviewee suggests that this could be addressed if the Internet security industry offered assistance to the public sector to disseminate knowledge that could be beneficial.

> A lot of the problem [on responses to cybercrime by law enforcement and the wider criminal justice system] happens because people don't understand the tech side of things. We [the computer security industry] have to educate the judiciary. I remember a case a while back about someone that got in trouble for hacking into some system. I could tell the judge had no idea how the hacking incident actually happened because of the stupid questions he was asking. (Independent #3)

The preventers of cybercrime may inadvertently cause deleterious effects, as highlighted in Chapter 6.4. Grabosky (1996) suggested crime prevention strategies could yield results that are unfavourable, and in certain cases, create a situation in which negative effects are unintentionally generated. It is clear that the criminalisation of crimeware has created a new form of crime. The prohibition of the distribution and use of crimeware may have inadvertently increased the value of certain crimeware tools subsequently creating a "black" market where such tools are made illegally available for sale and purchased for use. A reduced supply or availability of software used for the purposes of cybercrime may encourage the development of "private" tools. With a market for such software, this unintentional enticement (Grabosky, 1996) produces new creators of crimeware tools and technology for profit (p. 28). Furthermore, Sommer (2006) suggested that criminalising hacking tools "runs the risk of significantly inhibiting the activities of investigators, incident responders, penetration testers and academics" (p. 68). The perceived hubristic response to ban such activities has been contentious among the private Internet security industry. In the case of Germany, there have been reports of computer security companies withdrawing software products from the market that could be considered illegal (Thomas, 2007). An issue that has been raised in the UK related to the dual purpose of tools is that certain tools with legitimate functionality could be used for illegitimate use, and so labeled

as criminal. Certain tools that have useful functions for legitimate activities have been categorised as illegal due to its misuse (see Article 6 on KisMAC and Germany).

Crime prevention can also displace criminal activity. There is a form of *tactical displacement* (Bowers & Johnson, 2003, p. 276) whereby offenders alter their modus operandi. Similarly, there is a form of *resource displacement*, which is evident with the range of crimeware tools available that were selected by web forum site members based on its function and features. When one tool becomes ineffective, it was replaced by another tool. *Target displacement* was also evident which involves the selection of new targets if the original target is properly protected (Bowers & Johnson, 2003). In the web forum site interactions, targeting appeared to be indiscriminate, specifically in cases involving the attack and infiltration of websites, suggesting targets were mainly chosen among opportunities that provided the least resistance for the offender.

Criminal innovation is one feature of cybercrime that perhaps differentiates it from *terrestrial* forms of crime. For any sort of crime, innovation is presumed to occur over time with changes in the capacity of offending behaviour, the increasing or decreasing vulnerability of targets, and the capacity of those appointed to protect targets (guardians). However, crimeware tools and other forms of malware evolve at a comparatively rapid rate. Crimeware tools are updated sometimes within days of its release. With the development of new crimeware tools, some which mimic other tools and others based on distributed source code, the innovation is immediate and multiplied.

The link between offenders and guardians on the Internet could also be described as a rivalistic relationship. Cropley and Cropley (2011) suggested criminals to be "creative law breakers" that are in competition with law enforcement. Particularly for the case of the private Internet security industry, a struggle is apparent with guardians aiming to prevent cybercrime and offenders with the intention to engage in cybercrime. As noted previously, Ekblom (1997) alluded to the arms race occurring between crime preventers and those who commit crime. The endeavour to prevent cybercrime is difficult as it is offset by attempts by criminals to evade or circumvent efforts by guardians, which occurs as a cyclical chain of cause and effect, as raised in Chapter 6.4.

The approach to restrict software via criminalisation has existed for some time. In the US, the *Digital Millennium Copyright Act* (DMCA) contains provisions that bans "distribution of tools and technologies″ that circumvent copyright protection, which includes software. Problems with the DMCA have been ardently debated among liberal groups. A point of debate raised by the *Electronic Frontier Foundation,* an International non-profit digital rights group based in the US, warned that the DMCA would unfavourably hamper innovation and do little to stop the piracy of content as the act intended (Electronic Frontier Foundation, n.d.). It has raised concerns as to the adverse effects on freedom of speech, particularly in the US. Coleman (2009) argued that software could fall under principles associated with speech, freedom and liberal values. In the case of the US, crimeware tools could perhaps fall under the scope of freedom of speech.

The systematic surveillance of web forum sites may help anticipate trends with respect to crimeware tools, malware and associated activities. Monitoring such activities may not stop crime per se but online presence of law enforcement can perhaps deter cybercrime. Allowing *some* malicious and criminal activity to take place is one strategy. There have been a number of high profile cases of web forum sites that were monitored and taken down in the past by law enforcement.[157] However, such sites focused on activities directly linked to credit card fraud, not crimeware specifically. Disruption as a strategy by law enforcement did successfully shut down the carding sites nonetheless, it is uncertain whether such a technique would be effective with the possibility of the hosting of such sites moving to safe haven countries that tolerate certain online fraud activities. The shut down of sites may also displace sites to anonymous networks such as Tor.

Article 6: KisMAC and Germany

KisMAC is an open source tool widely used by security professionals, which allows users to monitor wireless connections as well as “crack” wireless passwords. In 2007, Michael Rossberg, the creator of KisMAC announced that he would no longer continue working on KisMAC due to the introduction of

[157] Two examples include *Carderplanet* and *ShadowCrew*. Both involved criminal organisations that persisted on web forum sites and were involved in credit card fraud activities. *Carderplanet* consisted mainly of Russian speaking members and was created in 2001. *ShadowCrew* was another site mainly composed of English speaking member that began in 2002. Both sites were shut down by law enforcement.

German law 202 that criminalises certain malicious software. As the law applies to Germany only, Rossberg has encouraged others outside of Germany to continue working on KisMAC. As stated by the Chaos Computer Club, a German based hacking community, “Forbidding this software is about as helpful as forbidding the sale and production of hammers because sometimes they also cause damage."

Article 6. *Lead developer of KisMAC calls it quits*. Retrieved July 10, 2012, from http://arstechnica.com/apple/2007/07/lead-developer-of-kismac-calls-it-quits/ (Berka, 2007)

6.6 Conclusion

A range of different actors with different motivations participated in discussions in the web forum sites from those with benign intentions to others with clearly illicit goals. The underground communities could be best described as a congregation of individuals with similar interests. Interestingly, the debate of the illegality of crimeware tools was discussed among the members on the sites. Questions were debated among members on the various types of crimeware considered to be illegal as well as the law, as was perceived by the members. Before embarking on examining the discussion data, it was not expected that such discussions would be openly discussed. In actuality, the criminality of crimeware was discussed among web forum site members, some of which conceivably include active offenders, leading to useful insight on how crimeware activities were rationalised on the web forum sites.

Viewing web forum sites associated with crimeware as a system which functions along other interdependent systems in the wider social order provides a unique perspective. There are, however, limitations of such a paradigm as systems theory approaches are difficult to test and are considered somewhat abstract focusing on society while ignoring individual action. Considering crimeware communities as a system illustrates its relationship with crime responders, which has potential implications for crime prevention strategies.

Chapter 7: Discussion and Conclusion

> Knowledge is twofold and consists not only in an affirmation of what is true, but in the negation of what is false.
>
> *~Colton*[158]

The goal of this thesis is to explore online offender communities involved in crimeware-related activities and to use the findings to advance the concept of the offender resource. The impetus of the study centres on understanding the social dynamics among the different actors linked to the distribution or use of software with malicious attributes that have increased risk for Internet users. This relatively recent phenomenon has professedly given rise to a new form of criminality, since mid 2000, and has been realised as a rather sudden transformation in the cybercrime landscape enabling and amplifying cybercrime caused by offenders. Software *designed* for crime, coined as crimeware, has as a consequence made cybercrime simpler to carry out and is now recognised as a common form of crime. The profusion of botnets, hacking incidents of websites and theft of online data are a few of the visible outcomes of the increasing prevalence of crimeware.

Before delving into the discussion points of the research, I will highlight certain background details while undertaking the journey of this thesis. The underlying interest, as a student of criminology, was to advance research on *active* offenders on the Internet. At the onset of the study, I noticed a lack of academic research on the social dimension of how offenders obtained criminogenic software tools. It was for this reason I began a preliminary investigation to examine the technical aspects of crimeware tools that I collected from the Internet and contacts in the industry. With an aim to identifying the important issues on cybercrime, I had spent a great effort, in regard to time and research funding, meeting with relevant industry practitioners around Australia and overseas, from the governmental, non-profit and private sectors, to find out about problems affecting Internet users. The industry reports from the private sector, reported statistics from government and past surveys

[158] Quoted from *Lacon* by Charles Caleb Colton (1820, p. 102).

highlighted different aspects of the cybercrime problem, but provided little insight on answering the question of *why* cybercrime occurs and what factors facilitate it.

Cybercrime is discussed as a growing concern in academic discourse, but little is known about cybercrime offenders. It is now accepted that crime follows opportunity (Grabosky, Smith, & Dempsey, 2001), however in the cybercrime scenario, such opportunity may only be embraced if the offender is appropriately resourced (Ekblom & Tilley, 2000). In the endeavour to learn about offenders and their behaviour, the earlier phase of the PhD was concentrated on seeking and exploring viable data sources for empirical analysis. Following this preliminary phase of the research, I decided to employ an observational methodology to analyse the web forum sites where offenders congregated. Having spent time interacting in chat rooms in the late 1990s amongst virus authors, I was curious to whether it had changed in the past 20 years and to explore linkages, if any, to the reported build-up of cybercrime in present day. Examining web forum sites where crimeware was developed and exchanged was the logical venue for investigation. It offered a source of empirical data for criminological research to better understand offender behaviour in their natural setting. The chief reason to study cybercrime was inspired by past experience and my academic interest in assessing theoretical explanations of cybercrime.

The research explored crimeware tools from three perspectives covered in the core chapters, which take account the learning dynamic among offenders, an examination of the offender as a rational decision maker (preceding crime), and finally the relativistic macro view of crimeware communities and society. The primary objective of this chapter is to advance the concept of the offender resource by connecting the findings from Chapter 4, 5 and 6, the core data chapters.

In criminological studies on cybercrime, resources used by offenders are addressed as a component of crime. However, it is not ordinarily discussed as an important factor of crime with its significance usually overlooked. Traditional crime scholars have often taken for granted that offender resources play a part in the act of a crime and place little importance on it as a subject requiring in depth inquiry. It was Ekblom and Tilley (2000) who first suggested in *Going Equipped* that in the endeavour to connect past explanations of crime,

investigating the resources used by offenders when engaging in crime may prove to be constructive. It was proposed that motivation alone was insufficient in realising a crime and that the offender would also need to have the means such as having certain skills, knowledge, technologies, or other implements before a crime could take place. Based on the investigation in the previous chapters, the research takes a further look at Ekblom and Tilley's (2000) theoretical emphasis on offender resources. The main objective in this final chapter is to recommend a feasible model to set apart the offender resource concept as a central point of examination, using the routine activity theory as a framework.

The subsequent sections will start off with answering the research questions, which correspond to the three core chapters (Chapter 7.1, 7.2 and 7.3). The latter two questions will focus on proposing a model of the offender resource concept (Chapter 7.4 and 7.5).

7.1 What are the online social dynamics and behaviours among offenders?

Explanations such as Sutherland's differential association theory posit that it is through social interaction that the values, techniques and motivations for criminal behaviour are acquired. It was evident that web forum site members engaged in cybercrime activities due to influence of online interactions with other members. Through discussions, members were able to learn how to use crimeware tools, techniques to evade anti-malware technologies, how to monetise their activities as well as observe the justifications of certain actions and motivations of other members. Additional social mechanisms that promoted learning involved interactions that encouraged certain offender behaviour. For example, the posting of tools for downloading that were difficult to find, provided utility or operational effectiveness, which were considered of value, were largely encouraged. Members rewarded actions that contributed to the circulation of such crimeware through positive responses. On the other hand, members snubbed or berated other members when discussion posts did not provide value, such as when out-dated crimeware were posted for download, or if a member, using deception, attempted to target the web forum site members themselves who downloaded crimeware for use.

Crimeware communities conceivably function as a virtual space for training, giving rise to new criminals. There was evidence of discussion threads that clearly catered to beginners. The ease of access to such sites increases the probability that, otherwise, law-abiding individuals could become involved in cybercrime activities. The observed interactions from seemingly new visitors coupled with the relative accessibility of the web forum sites supports Matza's (1964) view that criminals drift between legitimate and illegitimate behaviour, that is, under the presumption that such types of members were in fact new to the web forum sites and had not engaged in other forms of cybercrime previously. Moreover, malicious intentions may not always be a necessary motivation before an individual visits a web forum site. As motivations can be indoctrinated in the online social environment, motivations of crime can be learned and acquired over time, as posited by Sutherland, and may be less imperative as a prerequisite prior to the pathway to crime; in other words, the motivations of the potential offender can be formed after associating with offenders. It was unclear what originally drew new members to the sites, however, it was evident that the goals of those visiting web forum sites varied ranging from clear wrongdoing such as the hacking of websites to more questionable activities such as the posting of tutorials on how to deploy and use botnets. Burgess and Akers' (1966) extension of Sutherland's explanation of crime, which included the idea that peers could reinforce delinquent, and potentially criminal behaviours, was clearly evident in the interactions I observed. This reinforcement, simply a form of peer pressure, conceivably influenced other web forum site members to change their behaviours, motivations, actions and rationalisations towards crimeware. Such fundamental social dynamics are not exclusive to the offender. For example, reinforcement of behaviour due to peers is commonly used as the explanation of "peer pressure" in adolescence, and more generally this would also be in accord with Sutherland's view that the mechanisms of learning criminal behaviour are not exclusive to criminals.

There are consequences that relate to the spatio-temporal characteristics of the Internet (Yar, 2005) and the ease of access to web forum sites that are unique to the online environment. Access to knowledge, tools and other offenders are possible from any location where there is a computer with an Internet connection. The lack of space and time restrictions in the virtual setting of the Internet make online communities associated with

crimeware activities relatively accessible compared to terrestrial based criminal communities. The permanent nature of the discussion content also allows interactions to endure over a long duration and reach more people (generally, once a discussion post is made, is it is saved and visible to all web forum site members who can reply to the post). Face-to-face interaction at a specific point in time is necessary for "offline" interactions, however, it is not required for online interactions. In a manner, web forum sites are designed to function as learning environments. Additionally, if crimeware activities can be learned, the domain of potential offenders is much greater as any individual can learn the behaviours, knowledge, skills, techniques and motivations identified in the web forum sites. This was evident through the discussion threads that were aimed at new members.

Trust and reputation (as revealed in Chapter 4.4 and 5.4) also played a role in learning, although not specifically stated in Sutherland's differential association theory or the expanded version by Burgess and Akers. Von Lampe (2004) stated the first step in interactions among criminals is whether trust can be established. When describing the traditional mafia, Gambetta (1996) believed criminals within organisations were principally based on a platform of distrust and scepticism. Additionally, Gambetta (1996) described the buying of protection from the mafia as a possible alternative that obliquely satisfies the role of trust. On the web forum sites, it appeared trust could only be gauged based on one's past history of interactions and reputation. In *The Professional Thief*, by Sutherland (1956), it was suggested that reputation of a criminal, whether good or bad (from the perspective of criminals), dispersed through word of mouth to other criminals (p. 20). Sutherland's account alludes that interactions were not entirely grounded on distrust; assuming there were criminals with a positive reputation, and such actors would be perceived as trustworthy. The research indicated that trust and reputation played a key role among certain offenders, which also supports the findings from Décary-Hétu and Dupont's (2012) study on hacking forums. There was also evidence that suggests the reason a web forum site member would participate, when making useful discussion threads, was to establish their reputation. In other words, improving one's reputation was what drove further offender behaviour. For example, certain offenders requested others to provide "thanks" and "rep" for their discussion threads, which subsequently influenced how trustworthy the member was perceived among other members, as well as further encouraging the member

(who has the motivation to build their reputation) to participate via the creation of useful discussion threads.

The social ties and communication between criminals rely on the structural features of the surroundings that can decide the type of dealings that takes place. Van de Bunt, Siegel, and Zaitch (2014) described this dependency as "social embeddedness" in which interaction, mutual aid and simple communication among offenders ultimately hinges on where such individuals congregate or a common dominator such as a shared interest. The design of the web forum sites clearly indicated that multiple members were interacting within discussion threads based on a mutual interest. Within discussion threads, there were also cases in which web forum site members would collaborate on specific tasks. For example, the development of a new crimeware tool involved multiple actors in certain cases. Such instances consisted of at the very least two actors, the developer and the downloader (the user of the tool) who would sometimes provide feedback. For more sophisticated tools, there were more than two individuals involved and discussion content indicated stronger social ties with repeated interactions surrounding the author of crimeware. This would suggest a hub and spoke social structure (McGuire, 2012) with the hub being the author and the spokes including the "beta" testers, code sharers (those that contributed code) and graphics specialists to provide the visual "skin" for the crimeware. In cases when a specific service was provided, for example a malware spreading service, at least two individuals would be involved that would include the service provider and the customer. Such transactional interactions suggest brief and short-term arrangements with specialised roles, which correspond with Chabinsky's (2010) enterprise model highlighted in Chapter 2.5.

7.2 To what extent can offender interactions be explained as rationally driven processes?

Opportunity theories, more specifically the rational choice perspective of explaining criminal behaviour is useful in describing the behaviours of the members in the web forum sites. Inferred from discussions, offenders selected particular crimeware tools that offered the best chance of success in carrying out cybercrime activities. Specific tools were used to engage in particular activities. For example, not only were keyloggers purposely sought out

to siphon personal details from victims, but offenders also preferred to download certain keylogger "brands" and versions that were the most effective. When attempting to compromise computers on the Internet of unsuspecting victims, web forum site members used crypters to evade detection methods. Such actions signal a clear, and rational, decision that an offender's motivation was malicious as well as the deliberate action to avoid detection by "guardians" like anti-malware, other protection services and security professionals responsible for mitigating such activity. In the case of website hacking activities, it was the *weaker* and vulnerable targets that were more likely to be attacked, which also satisfies one of the key tenets of the routine activity theory that targets that lack protection are more likely to be sought out by web forum site members.

The distributed crimeware tools also indicated opportunistic behaviour, as certain tools were sold for a range of prices. Certain tools that provided specific functionality and stability, and that were less accessible, were more likely to be sold for a price rather than those made available free for download among web forum site members. Rationally driven processes were also manifest through the design and innovation of crimeware tools. For example, tools were continually fixed, improved and updated with new features. Such actions suggest rational behaviour as crimeware authors need to take into account information available, such as coding techniques aside from both attack and concealment features to incorporate in a tool, likely influenced from web forum site interactions, which then leads to the act of creating the crimeware.

With the availability of criminogenic software, knowledge, technique, and access to other offenders, the question arises where these align with respect to the causal steps of crime. Are already motivated offenders specifically visiting crimeware sites to engage in criminal activity? It is clear crimeware tools are precursors to other crimes such as online fraud and hacking activities, which suggest that involvement with such tools could be viewed as at least potentially *predicate*[159] relative to the actual crime. Furthermore, the ease of access to crimeware communities may play a role in inducing criminal activities. This raises another

[159] In US criminal jurisprudence, a *predicate* offense is a crime that precedes a more significant or greater offense. For an illustrative example, a predicate offense relative to the unauthorised access of a computer over the Internet would include the creation of crimeware such as a remote access trojan before it is actually used in the commission of crime to illicitly access a computer.

question, are potential offenders, who may have originally lacked the motivation to commit crime, subsequently engaging in criminal activity due to the acquisition of crimeware tools? The first idea would indicate opportunistic behaviour as selecting the proper tools for a crime requires a purposeful determination whether a tool is suitable, stable, safe to use and effective. However, the latter point of whether crimeware itself generates crime suggests that criminal behaviours may be acquired unintentionally or provoked, which follows that opportunity may have less consequence than social association with offenders.

Wortley (2001) suggested there are factors that may induce individuals to commit crime without which a crime would not have been committed (refer to Chapter 2.6 on Wortley's precipitators). As an example, Wortley (2001) described the influence that the mere sight of a weapon could have to activate feelings of hostility. An interesting point of contention is whether the availability of crimeware tools that are easily accessible is contributing to further crime. The availability of crimeware tools may prompt crime (Wortley, 2001), and so crimeware tools then play a crucial role as a *source* for crime for the potential offender that learns from other offenders. Crimeware is also a barrier to engage in offending activity, from the perspective of the offender who is predisposed to commit a crime; individuals, including criminals predisposed to commit crime, with little exposure to relevant technical knowledge or tools, could not commit such crime without the necessary resources. Cybercrime may be amplified by crimeware but there are basic obstacles for the offender, or potential offender, such as access to a computer, the Internet and relevant underground communities that subsist online.

Web forum site members, in certain cases, discussed the use of tools originally designed for legitimate use. It was clear that crimeware tools were available for different purposes, which produced a benefit for their users, including those with illegitimate reasons. Software made for legitimate use also paradoxically functions as a disruptive technology when used for the purposes of crime. This ambiguity of crimeware, whether legal or illegal,[160] was ardently debated among web forum site members.

[160] The web forum site members, in most cases, focused discussion on "legality", right or wrong in the view of the law, rather then whether crimeware and its associated activities were moral.

7.3 Where do online offender communities fit in the wider social order?

Online offender communities have both, from the functionalist perspective of crime, a contributory and unfavourable purpose in society. Functionalist explanations of crime would view communities that allow the development and access of crimeware tools as a normal part of society, which is permitted and expected according to Durkheim's view of the modern society.[161] Parallels may be drawn from rookeries in 18th century London where the criminal underworld resided and the poor lived due to unemployment (the equivalent of slums in present day), at the advent of the industrial revolution. Such squalid settlements were viewed as dangerous and regarded as the source of crime. In an essay on housing of the working class, Millington (1891) stated that, "vice and crime are created by these [rookery] surroundings … not entirely created by them [the criminals], they are perpetuated … [and are a] danger to the surrounding people [outside the rookeries]" (p. 48). In the same way, the existence of crimeware communities certainly poses risk to Internet users.

Crimeware communities that flourish also have certain utility. Malicious activities discussed within the web forum sites did contain discussions linked to the compromise of computers and incidents related to botnets, fraud and hacking activities that are clearly detrimental. On the other hand, the idea of certain aspects of cybercrime playing a positive role would appear to be contradictory. It is evident that the Internet security industry exists and provides employment based on the existence of criminal activities and use of crimeware tools by offenders. This evocation is not to show that crime is needed or serves a greater benefit, rather how crime serves a function from a macro-theoretical viewpoint. Along the lines of Elazari's (2014) immune system analogy as raised previously, hacking activities more broadly is a seemingly double-edged sword. It is also noticeable that cybercrime has had a great impact on the development of Internet infrastructure and systems subsequently influencing greater security in architecture and designs. To counter such responses, cybercriminals continue to invent new methods and deceptive techniques such as adapting social engineering methods when targeting victims.

[161] Described as "organic solidarity" by Durkheim (1891).

The decision to commit crime is based on how an individual confronts legal codes, the crux of Sutherland's differential association theory. The theory would suggest that if web forum site members viewed enough actions as favourable to achieve their needs, that is, actions associated with law-breaking or malicious behaviour, crime occurs as a result. However, if legal codes could not be discerned then criminal and non-criminal action would be difficult to discriminate, as offenders would not be able to distinguish the right and wrong of a particular action. Among the web forum site members, there was no clear demarcation of criminal patterns from non-criminal patterns as the interpretation of whether crimeware was illegal varied. Defining the favourability of legal codes is difficult if the legal codes are perceived as unclear among the web forum site members.

Grabosky (1996) suggested crime prevention under certain circumstances might unintentionally worsen matters related to crime. With cybercrime as an example of dysfunction in society, the growth of cybercrime certainly has manifest[162] or intentional outcomes. The response to crime is what allows such groups and institutions to exist and perform its tasks such as the development of new legislation that aims to ensure a safer society, jobs for law enforcement, the cybercrime industry that is focused on protecting Internet users, and the development of more secure Internet technologies. Eliminating all criminal activity is unrealistic. However, one option could be to implement a *triage* system to differentiate levels of harm, essentially classifying crimeware,, to more effectively address cybercrime prevention. For example, it may be more efficient to tackle higher risk most threatening crimeware first, and then move down the priority list. In this approach, society may be more equipped to respond to disruptive technologies. More effective strategies could be put forth if intent of certain software, the motivation of the parties that developed and released a tool, and the manner in which it is used in practice are considered.

Crimeware communities also have value for law and policy as they may prompt changes in society as new forms of criminality transform the “collective sentiments” (Durkheim, 2013) of society. An example of this would be the first countries to criminalise hacking software

[162] Merton explained manifest functions as the intended consequences where society is aware of the outcome. As a general example, the increase of social control is expected to decrease crime and deviance.

such as Germany and the UK. Criminalisation was a controversial response as it was disputed that it would adversely affect those in legitimate professions who investigate and analyse the tools and techniques of cybercriminals. The criminalisation of software is underway, yet still contested. It is opposed by computer security professionals for fear that it will reduce the useful role hacking has, hence the acceptance for techniques such as "reverse engineering" and investigations on crimeware. Both the lack of regulations or having too many restrictions in society can be harmful. Durkheim (2013) believed that crime, strictly speaking deviance and difference, was what compelled changes in society and helped to decide what shape the collective conscience will emerge. It was in Durkheim's (1893) doctoral dissertation *The Division of Labour in Society*[163] that crime was explained as arising due to the inability to manage the increasing specialisation and divisions in society. Simply put, it is harm that plays out as a result of this "structural deficit".[164] It was also expressed by Durkheim that modern societies tolerate differences better and that punishment should be proportionate to the crime with the goal to better the condition of society rather than overly punish it.[165] Parenthetically, the pervasive character of the Internet magnifies such differences. There is still great uncertainty and ambiguity in how to address online communities involved in crimeware activities; this may be part of the reason why certain jurisdictions have criminalised hacking tools while others have yet to address them. Overall, activities connected to "hacking" have increasingly become criminalised since the emergence of the Internet signifying a change in the social conscience and the recognition of direct and indirect harm from such activities.

As suggested by Merton (1938), deviant and criminal communities may result due to the disjunction of norms of the majority and the lack of ability to achieve success through legitimate means. Cloward and Ohlin's (1994) explanation expanded on this concept and described crime occurring if there were parallel illegitimate opportunities available and to

---

[163] *The Division of Labour in Society* was originally published in French with the title *De La Division Du Travail Social*.

[164] In this context, *structural deficit* describes the gap, confusion or chaos that can occur in society due to change.

[165] Durkheim used the terms "mechanical solidarity" and "organic solidarity" to refer to the basic primitive society and advanced modern society respectively. In the extreme case if we view current responses to cybercrime as punitive, this would suggest society at present reflects the basic primitive stage. If today's society is more reflective of the advanced modern form, punishment would be more restitutive. In either case, it is modernisation where crime originates.

realise such opportunities the potential offender would need to learn from other offenders. Also extending Merton's explanation, Murphy and Robinson (2008) suggested that certain individuals choose to engage in *both* legitimate and illegitimate pathways to achieve success. All such explanations conceivably describe the formulation of the web forum site communities. As a result of the inability to achieve success in society, individuals join crimeware communities as an alternate way to achieve their goals such as the pursuit of profit, as well as to develop particular skills and knowledge relevant to crimeware. Additionally, actors who have the motivation to engage in cybercrime prior to joining such sites may be doing so as both legitimate and illegitimate may not be available – this would imply web forum site activities fall somewhere in between non-criminal and more organised serious forms of cybercrime. It follows from such a view that web forum sites are not necessary in all cases to learn the motivations of criminal behaviour. Rather they may play an ancillary role in the indoctrination, through online social interaction, of criminal behaviour if other pathways to learn crime patterns are available. Murphy and Robinson's (2008) explanation would imply that a single person could be both a criminal and a non-criminal, which to some degree was evident in the case of two of the interviewees who were former *black hats* that ceased their cybercrime activities after progressing into legitimate roles in the Internet security field.

Institutions such as law enforcement benefit from increased policing powers associated with new cybercrime legislation. The Council of Europe *Convention on Cybercrime*, which was developed to improve techniques for investigation and cooperation among nation states, contains a clause that effectively bans such tools.[166] The Convention is an example of a legal instrument that has increased the capabilities of law enforcement, that is, for countries that have put into effect relevant legislation. On the other hand, proponents of conflict-based explanations of crime would view crime as the product of a clash between society, for instance those in power and crimeware communities. Examples of the powerful elite include groups, businesses and institutions with power to influence authority. Other bodies include policy makers that function to address public needs, financial institutions and banks that are often the victims of cybercrime, and the "for-profit" Internet security

[166] According to Article 6 of the *Convention on Cybercrime*, signatory countries shall criminalise certain types of software used for crime. Refer to Chapter 6.1 for further details.

industry. New laws and the criminalisation of crimeware could also be viewed as an outcome of such conflicts.

For the case of Internet organisations that respond to cybercrime activity, the relationship is more complex. For example, the private Internet security industry certainly does have conflicting interests as their goal is to remediate and prevent cybercrime, but they also gain from criminal activities as they benefit from providing solutions to remediate those same problems. Additionally, by exposing certain techniques and patterns of cybercrime, as was mentioned in one interview, the cybersecurity industry influences offender behaviour as the tactics to stop cybercrime are pre-empted by offenders creating a sort of iatrogenic cycle. The larger ecosystem that consists of crimeware communities, crime preventers, law and the Internet security industry is intricate, with necessary dependencies that are not always beneficial.

7.4 How do the selected theories in the study interconnect to explain the online behaviours examined?

The focus of this section is to explain the logic behind the three conceptual models of offender resources presented in the next section, Chapter 7.5. The three proposed models have been constructed based on the theoretical viewpoints of the core chapters. In comparison with a true theory integration, this research works toward a definitive theoretical *starting point* by exploring multiple explanations of crime that are traditionally considered distinct. The benefit of using multiple explanations of crime is that it allows different levels of analysis that may have differing assumptions. Relying on more than one theory can also be beneficial in highlighting the useful parts of the different theories and bringing them together. Another benefit of working toward integrating theories is that it helps to elaborate on a concept where a single theory alone may not be sufficient as an explanation for crime. Before theories can be properly integrated (e.g., through empirical testing and finding conclusive relationships between propositions from different theories), they must first be considered individually and connect conceptually (simply put, we

consider whether certain theories are useful).[167] To reiterate, the thesis does not explicitly test theories nor does it empirically integrate theories using quantitative methods, in spite of this it does nominate certain explanations, models and theories from criminology and raise possible linkages.

In Chapter 1, the routine activity theory is used as a framework to develop the concept of the offender resource, namely crime facilitators in supply at hand to the offender such as tools, techniques, knowledge, skill, motivations and other offenders, that are used in the crime commission process. In this initial model, the offender resource element is shown as an additional requisite of the routine activity theory (see Figure 8 in the next section). That is, offender resources are distinct from the offender, target and guardian.

The first proposed model emphasises the offender resource concept but centres on the offender (see Figure 9 in the next section). It draws from the findings in Chapter 4 where the point of investigation is on the learning activities of web forum site members. This model stresses the importance of the role of the offender.

Also relying on Chapter 4, the second model underlines the offender resource concept but incorporates how it changes over time relative the offender (see Figure 10 in the next section). It also draws from the findings of Chapter 5, which reveals that online interactions were driven ultimately to maximise benefit, which can include building one's reputation, the successful compromise of a target, or the accumulation of items of value such as money, stolen data and crimeware. Offender resources are presumed to precede the event of a crime with *social learning* coming before the routine activity theory.

The third model focuses on the macro dimension of the routine activity theory. In fact the routine activity theory was originally proposed as a macro-level theory to explain victimisation rates (Cohen & Felson, 1979). The routine activity theory presumes criminals

[167] The theory integration process is presumed to take place in two general steps: the first is a conceptual integration (argument whether it makes sense to combine more than one explanation of crime, and subsequently explore how this could be done) and the second phase involves empirical integration using quantitative techniques (identifying correlations and connecting propositions of different theoretical explanations). This thesis focuses on the first step.

to be rational, opportunity-maximising individuals, a theme explored in Chapter 5. The function and role of crimeware communities relative to other groups in society is the focus of Chapter 6. This model emphasises the societal dimension such as crimeware communities as a social group. This model connects the findings of Chapter 5 and 6, and offers a view of offender resources as a part of a larger social system (see Figure 11 in next section).

My original goal before embarking on this thesis was to propose a singular unified model of the offender resource concept. The focus was on exploring the events that precede more widespread forms of cybercrime such as fraud, theft and related hacking activities. To reiterate, cybercrime linked to ideology or of a political nature was not covered. Trafficking crimes for instance the trade of drugs online, and content crimes such as the distribution of material related to child abuse was not investigated. Combining an excessive number of explanations that span different traditions of criminology, even while focusing on only one general category of cybercrime, over complicated the conceptual model. For this reason, I have decided to present multiple conceptual models of the offender resource. To stress, the models are intended to be abstract, as it is a representation of a concept and not a prescriptive theory. The following section will re-examine Ekblom and Tilley's conceptualisation of the adequately resourced offender, with the three conceptual models presented after. Along with examples, important theoretical implications and corresponding potential crime prevention strategies of the conceptual models will be presented. The underlying goal of the research was to stress the importance of offender resources as a theoretical concept in the etiology of crime. The objective of the following section is to conceptualise how best to explore crimeware as a topic of inquiry in criminological research. The conceptual models presented in the next section are abstract but pragmatic that show what an offender resource model could look like based on the data examined. Each model is simply a guide and is not meant to capture all aspects of the offender resource concept.

7.5 What is a feasible theoretical model that describes offender resources?

The routine activity theory states a crime occurs when a motivated offender and a suitable target meet where there are no capable guardians. In Ekblom and Tilley's (2000) extended view of the theory, additional requirements are also needed one of which includes the adequately resourced offender. They stated that resources play a role in the offending process. These included a target that was vulnerable, the absence of crime preventers, the presence of crime promoters,[168] the physical environment had to be suitable for the offender and crime promoters, and most importantly the offender that is adequately resourced to commit the crime.

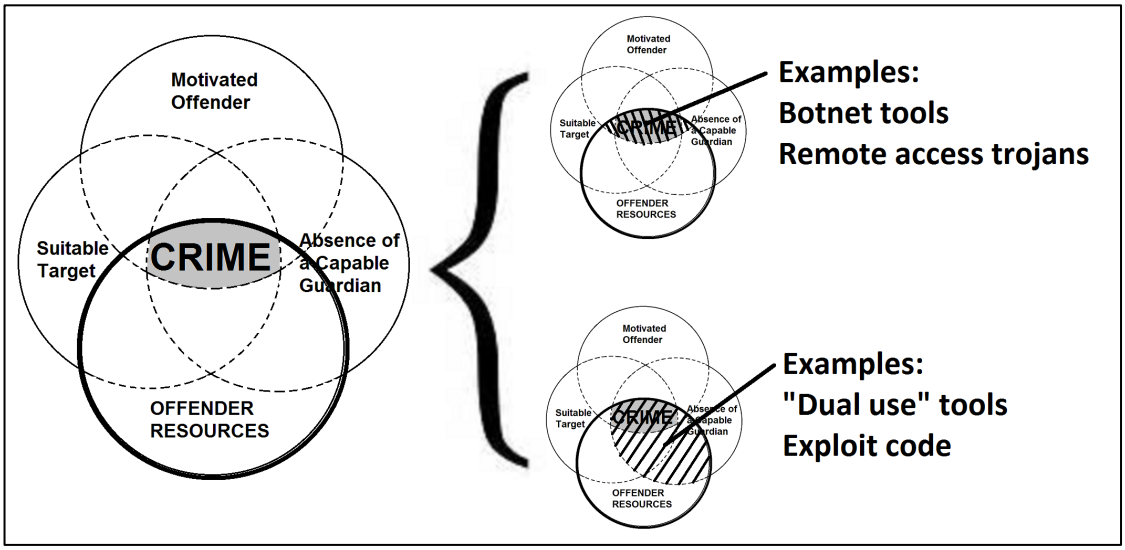
Revisiting the model posed in Chapter 1 that focuses on the idea of crime occurring at the junction of such elements, offender resources was presented as an additional requisite of convergence (see Figure 8). This conceptualisation of the event of a crime emphasises the various elements that need to intersect. Offender resources in such a case would be any item in supply and accessible to the offender. Examples from the data in the research include certain crimeware such as freely downloadable remote access trojans, specific skills required to make customised tools such as crypters, and access to tutorial and instructions on how to use crimeware. Crime facilitators such as co-offenders or other individuals that make crime easier (crime promoters) would also fall within this offender resource depiction. Offender resources also comprise knowledge of cybercrime techniques, which is often propagated in the form of information that is transferred on web forum sites. As was indicated in Chapter 5.3, there are certain resources that are used by offenders that may also be employed by "guardians" (highlighted in Figure 8 as "Dual-use tools"). There are certain tools that have utility for legitimate purposes that can also be used for crime.

The findings also have theoretical implications for the conjunction of criminal opportunity (CCO), also developed by Ekblom (2005), which was introduced in Chapter 2.8. CCO conceivably is an extension of the offender resource concept from Ekblom (2001), as it addresses *resources* as a distinct concept in the crime causation process. Offender resources are implied in point 4 (there are 11 preceding factors of the criminal event) in the model, which takes into account resources at hand to the offender. Furthermore, the complete CCO

[168] Ekblom and Tilley (2000) described crime promoters as individuals "making crime more likely by shaping the situation or influencing the offender" (p. 379).

(all 11 factors, not limited to point 4) emerges as a potential model to address offender resources, if offender resources are interpreted to extend beyond simply software but also include websites, communities and people. The *predisposition to offend* can be acquired as motivations and actions can be imitated and learned through online interactions. The *lack of resources to avoid crime* is indicated to some extent, as certain web forum site members did not view the law as an obstacle when employing the use of particular crimeware. Some individuals are more likely to be influenced and engage in malicious activities as they spend more time on the sites, which may affect their *readiness to offend*. There are certainly varying skills, knowledge and software being disseminated on the web forum sites, which function as *resource for committing crime*. The *decision to commit crime* can be inferred as websites were posted as potential targets; these sites were posted based on its characteristics, for example, weaker unprotected websites were listed in discussions, which plausibly serve to prompt a criminal response. An example of *offender presence in situation* is clear as multiple individuals posted in discussion threads conversing on different topics related to crimeware, botnets and hacking. *Targets* mainly comprise systems accessible over the Internet, which indirectly affect its owners whether that includes businesses or general Internet users. The *target enclosure* in the Internet scenario consists of intrusion detection systems and firewalls that aim to block activity generated from crimeware. The *wider environment* of the Internet is arguably conducive for crime as it can provide anonymity, for example via botnets, proxies and VPNs. *Crime preventers* are the businesses in the computer security field that build products that aim to prevent cybercrime. Lastly, *crime promoters* are made up of actors such as the experts, the highly skilled that offer certain cybercrime services (for example, crypter services) and the members that sell crimeware tools (examples are provided throughout Chapter 5). As the CCO offers possible intervention points for each of the 11 causal factors, practical crime prevention strategies can be deployed tailored to each cause.

Figure 8: Offender resources as a 4th element based on the routine activity theory



A case example, which demonstrates the model in Figure 8, of *offender resources* that intersect the *motivated offender* includes the 2012 case of Edward Pearson who was arrested in the UK for online fraud after stealing online login credentials for approximately 200,000 PayPal accounts along with other personal private information from numerous victims (Vinter, 2012). Pearson was alleged to have used two popular crimeware kits explicitly designed for cybercrime known as *Zeus* and *SpyEye* to unlawfully accrue data from his victim's computers. In this scenario, the tools *Zeus* and *SpyEye* exemplify offender resources. As covered in Chapter 5, there also exists software that is sometimes grouped under the "crimeware" umbrella with features that have legitimate purposes. An example of such tools includes port scanners that probe networks for security holes that are used for both legitimate and illegitimate use. These "dual-use" tools are not designed specifically for crime but can potentially be used for nefarious purposes by the motivated offender. For this reason, certain software can get grouped under the "crimeware" umbrella with features that have legitimate purposes (see Article 6 on KisMAC and Germany). As an additional element, the conceptual representation of offender resources is shown as a component of crime that must converge along with the motivated offender, suitable target and lack of a capable guardian.

Continuing the discussion on crime prevention in Chapter 6.6, strategies to address crime could centre on preventing the availability of offender resources by disrupting access to the

web forum sites where crimeware can be accessed. It has been suggested one method to reduce crime is to restrict the resources for offending (Gill, 2005; Cornish & Clarke, 2003). A presumption can be made that removing this additional element of convergence would reduce the opportunities for the offender, as crimeware required to engage in cybercrime would be unavailable. By impeding the access of resources from offenders, the presumption is that this would decrease crime. As a potential *pinch-point* to prevent crime, restricting crimeware tools seems to be a logical approach. One straightforward example is the shutdown of its source such as a web forum site, as was the case of *VX Heavens*.

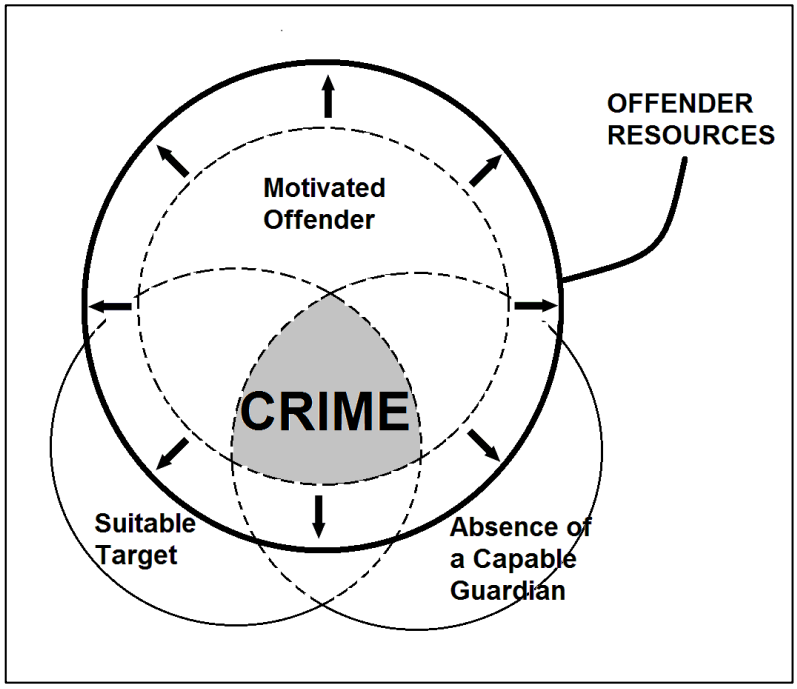
Revisiting CCO, the framework proposes 11 causal factors with corresponding intervention strategies. To tackle the more immediate causal factors, perhaps regulation of online behaviour is one possible strategy. For example, this could be done if web forum sites disallowed certain discussion threads from forming such as botnet tutorials that may work to inspire and encourage criminal disposition of new members (1. in CCO model). Rather than blocking certain discussion content, another possibility is to "direct" members by limiting access to certain discussion groups, or perhaps *dummy* systems can be deployed online that function as practice grounds where malicious activities are diverted (6. and 7. in CCO model). Notifying vulnerable sites as soon as they are listed in a discussion thread would certainly give them time to remedy weaknesses (8. in CCO model). As covered in Chapter 6.3, the skills of web forum site members can be used for both positive and negative purposes. Another tactic is to lure highly skilled individuals to help mitigate crimeware activities that may otherwise engage in cybercrime, and collaborate with crime preventers (11. in CCO model).

In situational crime prevention, Clarke (1997) separated crime prevention approaches into three categories: degree of surveillance, target hardening, and environmental management (p. 223). Cornish and Clarke (2003), expanding on these categories, suggested 25 techniques to reduce crime, which largely prevents offending activity by increasing *friction* between the motivated offender and the target. Reducing the availability of resources used to engage in crime, which is taken into account in one of the 25 techniques of situational crime prevention under "control tool/weapons", is contentious as how this can be employed in practice without inadvertently affecting legitimate users is uncertain (e.g., through

criminalisation). Obstructing or stopping offenders from accessing such resources as a response to cybercrime may reduce the likelihood of crime. However, such a strategy may also adversely affect guardians. As offenders adapt to crime prevention responses, it is possible the web forum sites could be pushed further "underground", for example safe haven countries or the Tor network. In this hypothetical scenario, it would be the crime preventers that would be adversely affected.

The first model proposes a different version of the offender resource concept from the previous that focused on the idea of convergence (see Figure 9). Offender resources are coupled to the motivated offender in the following model. The motivated offender and offender resources may also be viewed as having a biconditional relationship, that is, both elements co-exist. In contrast to the original routine activity theory, the emphasis is placed on offender resources that derive from the motivated offender. Offender resources should not be viewed as "tangible" crimeware items that can be banned, rather it is recognised as things that stem from exposure to crimeware. For instance, offender resources can include *expertise* on how to setup and deploy specific crimeware such as *Zeus* or it can consist of the *knowledge* to monetise botnets such as click fraud. It can also include *reputation* as perceived among other offenders or *relationships* with collaborators. This model also posits that motivation without resources is insufficient for the offender to engage in cybercrime, which differs in emphasis with the previous model (referring back to Figure 8) where the offender may have available the choice of a plethora of crime enablers and facilitators when engaging in cybercrime.

Figure 9: Offender-centric offender resources based on the routine activity theory



A case example, which demonstrates the model in Figure 9, *Butterfly Bot* was a bot crimeware tool that was designed for the explicit purpose to illicitly monitor and steal passwords from computers of unsuspecting victims. Between 2008 and 2009, the tool was also known to have been responsible for the creation of the *Mariposa* botnet consisting of approximately 12 million compromised computers, which was controlled by a group that called themselves DDP Team (Corrons, 2010).[169] The *Butterfly Bot* tool itself was originally created by a Ukranian hacker who went by the alias Iserdo (Krebs, 2015). Iserdo had allegedly sold the tool to the DDP Team who used the crimeware to engage in activities related to the *Mariposa* botnet. In this scenario, the offender resource is demonstrated as the *relationship* between the DDP Team and Iserdo, with the motivated offender as the DDP Team.

This model implies that the banning of certain crimeware may be an effective approach, as forbidding knowledge, or relationships with the creators of crimeweare, is difficult to enforce. The model would also elect that offenders seeking access to particular resources,

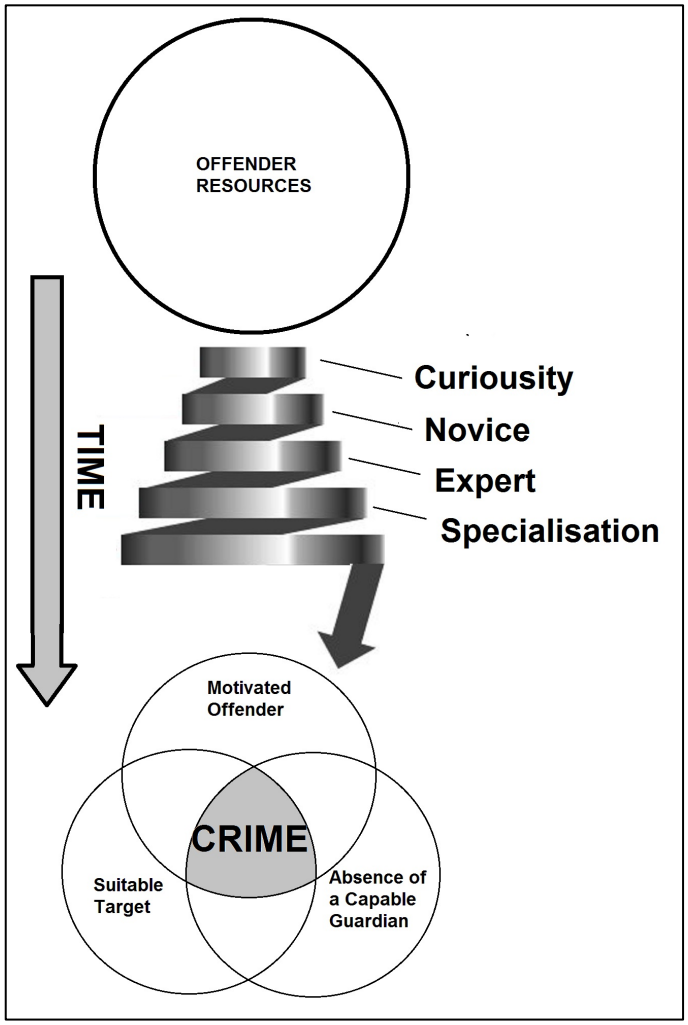
[169] *Días de Pesadilla Team* is Spanish for Nightmare Days Team.

who are already motivated and predisposed to committing a crime, may not be capable to engage in cybercrime without the proper resources.

The second model emphasises the learning dimension. Ekblom and Tilley (2000) suggested that in the decision making process of offenders, the choice to use particular resources factors into the decision making process when an offender rationalises whether to commit a crime. This maintains the assumption of offenders as opportunistic and rationally thinking individuals. As suggested earlier, crimeware tools may also precipitate crime, and the ease of accessibility of the tools itself inducing crime to occur. Also stated previously, the acquisition of crimeware involves processes reminiscent of learning, which takes place over a period of time. The "motivated and adequately resourced" as implied by Ekblom and Tilley (2000), which draws from the "motivated offender" from the original routine activity theory, focuses the attention on resources in connection with the offender. As revealed in Chapter 4, there is support that learning through interaction with offenders can play a role in the process of becoming an offender. The convergence of the three elements of the routine activity theory brings about crime, however in the cybercrime scenario, individuals must first acquire the attributes of the offender, and this occurs through social processes indicative of learning. This process is not immediate and occurs over some duration of time (see Figure 10). This increasing intensity of social engagement with offenders online is highlighted as “curiosity”, “novice”, “expert” and “specialisation”. The more frequently an individual visits, participates and engages in activities in online crimeware communities, the more likely they are to engage in cybercrime activity at a subsequent time in the future.

Motivation may be formed through interaction among offenders and the offender may exhibit rational qualities, however it is the past association with offenders that is a key factor leading to the criminal event. This would address one of the limitations of routine activity theory that assumes the offender is motivated but does not explain how motivation is developed. Motivation can be acquired and indoctrinated in the online environment of crimeware communities (as stipulated by Sutherland in his differential association theory).

Figure 10: Offender resources, time and the routine activity theory

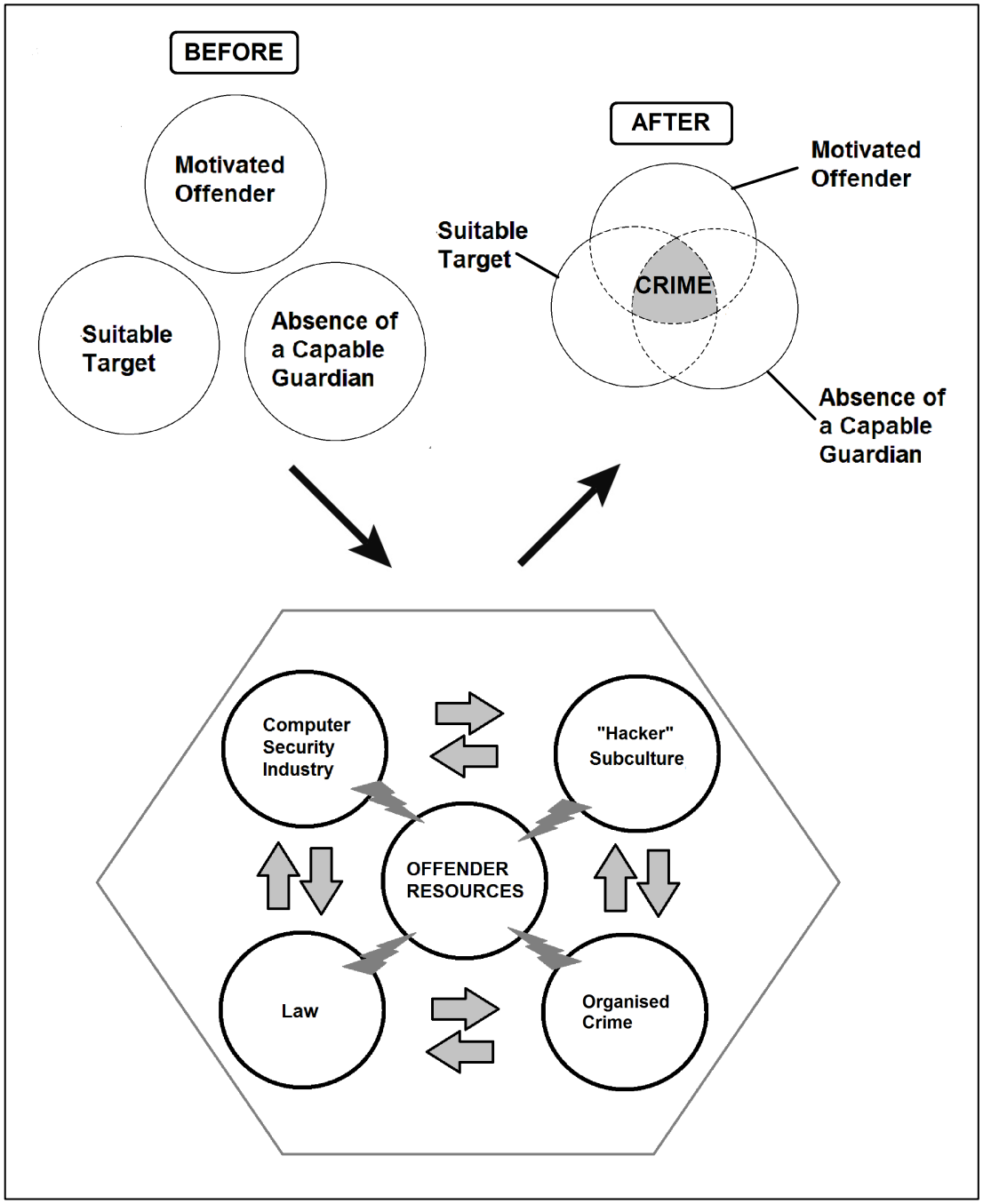


A case example, which demonstrates the model in Figure 10, can be illustrated with the 2015 shutdown of the underground malware marketplace known as *Darkode*. It was alleged that the site had 300 active members who were engaged in various fraudulent activities. According to the investigation by the US Department of Justice, "prospective members were allegedly vetted … to the forum for the purpose of presenting the skills or products that he or she could bring to the group" (US DOJ, 2015). In this instance, the process of vetting and revealing one's skills conceivably occurred over time where continual interactions were required with potential members needing to prove their value to the group.

One implication of this model on crime prevention, or a possible strategy, is through the plausible connection between the reduction of cybercrime and the re-focus of the learning process if channelled to more constructive endeavours. For example, generating more jobs and hiring former hackers in the field of Internet security, with the goal to attract the potential offender, current or past offenders, may work to "redirect" cybercrime and also improve the capacity of crime preventers.

Another conceptualisation of the offender resource concept focuses on the idea of crimeware communities as a social system that has a function in society, which connects to other groups, systems and institutions in society (see Figure 11). An implication of this conceptualisation is that the online communities involved in crimeware activities have a certain role in the social order, and are needed by other groups, systems or institutions to operate. This mutually dependent relationship was explored in Chapter 6.4. The model proposed is rather abstract but the central point is the multifaceted relationship offender resources have with multiple agents (for example, the computer security industry and cybercrime legislation) with offender resources preceding the event of the crime (as opposed to it being criminal in itself).

Figure 11: Offender resources as a system relative to the routine activity theory



A case example, which demonstrates the model in Figure 11, can be shown through the password finder tool known as *CloudCracker* that was at one time available for sale for $200 USD. The tool had the functionality to eavesdrop on encrypted network traffic via a VPN and identify passwords being sent that have been erroneously transmitted in an unencrypted format. According to an interview with its creator, the intention of the tool was to "force people to use more secure VPN technology in the products they are building"

(Finkle, 2012). It is certainly possible those with criminal motivations as well as legitimate professionals may use such tools. It is also likely this event has prompted the Internet security industry to improve current VPN technology.

Deterring the development and use of offender resources like crimeware or the access of crimeware communities could foreseeably prevent crime, however, other systems depend on activities generated from crimeware communities. In such a case, categorising crimeware and its associated activities may be constructive through a form of social control. Crime prevention strategies based on this model may involve some form of regulation, for example, explicitly permitting the access of crimeware tools, such as an individual working in legitimate industry. Additionally, a potentially constructive social control measure could include web forum sites that are controlled by independent bodies. Crimeware in a manner would be permitted but monitored. It is clear from the findings of the research that convergence may describe the development and distribution of crimeware, but insufficient as an explanation for cybercrime.

7.6 Future Research

The future research suggestions in this section centre on ways to better understand the offender. Some of the following points were briefly mentioned in the methodology presented in Chapter 3. In the onset of the research, offender engagement through interviews with web forum site members was planned as a second phase to the study. Unfortunately due to time limitations of PhD research, this subsequent part of the study was not carried out. Offender interviews may have provided additional data to determine motivation from the point of view of the *active* offender implicated in cybercrime activities. Further insight into the offender decision-making process involved in the development and access of particular resources could have been captured. There are also potential safety concerns to the researcher and potential backlash when interviewing active offenders that may pose a risk. Although only occurring in exceptional cases, researchers that have directly engaged with certain offenders have been threatened in the past (Jacques & Wright 2010), which is always a possibility dealing with cyber offenders.

Offender interviews could also provide the data to possibly *anchor* routine activity theory to other criminological theories concerned with social forces that drive offenders to commit crime. Criminal behaviour may be learned through online interactions, as demonstrated in this thesis, but there may be other relevant factors in the terrestrial environment of the offender. Although typically taken as a given, the routine activity theory by default presumes at some level the offender is rational (routine activity theory is often considered an offshoot of rational choice). That is, the offender would need to decide whether to engage a victim and guardianship is insufficient enough to take the risk. Incorporating other theories on offender motivation may provide greater explanatory power, which reveals insight into other topics associated with "cybercrime" such as cyber-terrorism and hacktivism (ideologically motivated hackers) with seemingly different underlying motivations. CCO is reasonably amenable as a framework for offender resources that perhaps can be extended to the case of cyber-terrorism. According to Ekblom (n.d) there are variants of CCO dealing with terrorism (and the drug trade); CCO could be further expanded, if needed, to explore the *cyber* equivalent of terrorism. While the routine activity approach provides great insight, it can limit the choice of theoretical explanations from criminology to draw from, if the *motivated offender* is accepted as a given without question.

Future qualitative studies on web forum sites in other languages may be of interest for criminological inquiry and a way to obtain additional insight into offending behaviour. As cited throughout this thesis, Holt (2013) examined Russian language forums relevant to stolen data and different types of malware. Décary-Hétu and Dupont (2012) investigated a single web forum site involved in botnet activities, which is presumed to be English language-based. Other languages of interest include Chinese, Korean, Japanese, Spanish, German and Portuguese (Brazil), languages of relevant countries with a high Internet penetration rate or population. It is uncertain if web forum sites would be the venue of choice among offenders of other languages, or whether "crimeware" communities exist at all. A former Chinese law enforcement colleague of mine that has dealt with hackers in China had once mentioned that such communities do exist in China under the guise of legitimate online computer security forums. It is speculated here that norms and social

patterns among online cybercrime communities of different languages would be more or less similar, but this would require further empirical investigation.

Investigating *changes* or *comparing* web forum site interactions over time may be worthwhile for researchers interested in understanding how behaviour transforms over time and the development of new forms of criminality. The exploratory *cross-sectional* approach used in this research relied on a modest sample of web forum site discussions, which may not be representative. A longitudinal approach may help researchers to identify whether the findings in this research are temporary short-lived occurrences or a long-term phenomenon. A possible valuable point of investigation could be to compare web forum site activities, similar to the sample examined in this research, with Usenet newsgroup activities from the late-1980s and early-1990s. Usenet newsgroups are predecessors to chat rooms and web forum sites common today and have been known to contain hacking related discussions, for example, the alt.hackers newsgroup. Old collections of Usenet newsgroup interactions have been archived and are accessible; a study is certainly possible to accomplish. Notably, crimeware, as identified in this thesis, did not exist 20 years ago. However, malicious code, traditionally referred to as viruses were once widely accessible on Usenet newsgroups. Parallels may exist between present day activities and those that occurred in the past, which could be a promising approach to explore the evolution of cybercrime. With the scalability of botnets and cybercriminals that continually innovate, it is likely to escalate risk in the future with the increasing dependence of devices that rely on the Internet. The *Internet of Things* will expand our reliance on technology that interfaces with the Internet from wearable devices that monitor our health to smart security systems that safeguard our homes.

The social dynamics, norms and activities within *closed* communities could potentially be different. As the research focused primarily on publicly accessible web forum sites involved in crimeware activities, it may not be representative of all activity although an effort was made to obtain a mixture of samples. More elusive smaller online communities, that may have certain conditions for registration and potentially more difficult to access, may reveal distinctive activities and pursuits among their members not found on larger sites. The association among members in these communities may be more closely knit with

prolonged interactions as there are less people. I would hypothesise these smaller groups would fit the more traditional models of "organised crime" with more cohesive group structures, as opposed to the loose and somewhat disordered "one-off" relationships observed on the larger public web forum sites. As a follow-up to this thesis, the next endeavour is to measure the strength of links between the actors participating on web forum sites taking into account their roles.[170]

An effort to catalogue crimeware tools distributed could be of value for study. The systematic and ongoing collection of crimeware, viruses and other forms of crime-relevant software could be beneficial if one wanted to study its technical characteristics at a subsequent point in time. While carrying out this research, I found it difficult to find versions of certain tools that were older than four years old (pre-2007). It is likely copies of older software will become less accessible as they become less effective for cybercrime offenders. The availability of such a repository could benefit crime prevention and Internet security response agencies. It is probable Internet security companies do collect such software, but it is unlikely to be shared.

There are ideal approaches when undertaking academic research. Adopting a more quantitative research design, the use of probabilistic samples would conceivably allow for generalisations to be made of the larger population of web forum site participants. Yet, collecting a true random sample of web forum sites is fundamentally unachievable as the "universe" of web forum sites is indefinite and constantly varying. In a seminal study by Holt and Lampke (2010), which has been influential in this thesis, web forum sites containing discussions on the exchange of stolen personal private information and financial data were identified using Google search and sites posted by forum participants. Although not a probabilistic sample, it was a sensible and practical approach of identifying sites and to investigate buyer-seller relationships and market dynamics. A forerunner of criminological empirical research of online populations, Holt (2010) outlines the numerous limitations and challenges of "non-participant" qualitative research of data collected from online platforms where offender populations congregate - an invaluable *must read* guide for

[170] This research project has commenced and explores web forum site data acquired from third party organisations.

future researchers. In this thesis, the selection of web forum sites identified via online polls (with one site added from Tor) that were methodically analysed certainly does not allow to generate statements that describe all online offenders involved in nefarious activities, but does provide a platform - that is both pragmatic and sufficient - to investigate the offender resource concept. Moreover, the interviews, cases (electronic data) and articles offer a frame of reference to help grasp the relevancy of the findings from the viewpoint of data *in the wild* and crime preventers.

7.7 Final Remarks

The goal of this thesis is to expand on a current field of knowledge and explore various explanations; however the underlying aim is to raise further challenging and relevant questions. Researching the topic of cybercrime is an ongoing investigation as the field is constantly evolving, and with the rapid speed of technological advancements, new forms of criminality are bound to develop. New theories, methods and techniques in criminological research are expected. Nonetheless, it may be suggested that the most effective approach is to study the fundamental issues. I posed the question at the beginning whether cybercrime is different from crime before the Internet. The empirical data supports that it is certainly unique, though with many similarities. I conclude that early explanations of criminal behaviour are just as relevant today as when they were first posited.

Appendix 1: List of crimeware

0x88	BioZombie	Cybergate
1337 Steam Stealer	Bitching Threads	Cythosia
541's Keylogger	BKB Keylogger	Daemon Crypt
A++++	bLacCkOut Keylogger	Daleth RAT
A32s	Black Oil	Dark Booter
Acunetix	Blackhole	Dark IP Stealer
Adpack	BlackNix	Dark Moon
Aegis Crypter	Blackshades	Dark Screen Stealer
AIO	Bleading Life	DarkComet
Aircrack	Blue Banana	DataGuard AntiKeylogger
AirSnort	Blue's Port Scanner	Dcrypter
Albertino	Bobup Scanner	DD7 Port Scanner
Albertino Keylogger	BracoLogger	Deeper RAT
Amnesia	Brutus	Deh Crypter
Amok Joiner	Bytes Adder	DejaBooter Stresser
Angry IP Scanner	Calypso Logger	Dekoder's Crypter
Apocalypse	Carb0n Crypter	Devil Shell
Arabian-Attacker	Cerebrus	Digital Keylogger
ARC	Char0n	Divine Stresser
Archelaus	Chrome	dnsniff
Arcom	Chronic	Doctor Logger
Arctic R.A.T.	CIA	DR VBS
Ardamax	CigiCigi Binder	DUH Logger
Armitage	Citadel	Duh Logger
Assassin Crypter	Click	Easy Binder
Aura Stealer	Comradex	Easy Crypter
Avenge Stresser	Coods Cryter	Eclipse Booter
Award Keylogger	Cool Anonymous Joiner	EES binder
B!kA LoggeR	Core Impact	EgySpy Keylogger
Bandook RAT	Cracked On The Fly	El Bruto Crypter
BattlePong	Crimepack	Emissary
Beast	Critical Stresser	ettercap
Beast	Cry217	Exploit scanner
BFF DoS	Curiosity	Fiesta Pack
Bifrost	Cyb3rK3yl0gg3r	File Injector

(...continued on the next page)

File Joiner	ISR Stealer	Midnight Stealer
Fileprotector	ISS Internet Scanner	MiniMo
Final Fortune	iStealer	miniRAT
Firefox Password Stealer	iStealer	MLV Crypter
FKS	iTeam Crypter	Modest Keylogger
Flux	J-Logger	MofoTro
Fly Crypter	J.E.T. Keylogger	Mpack
Fresh Keylogger	Japabrz' Csharp Crypter	Multi Password Stealer
FreshBind	John the Ripper	Multisploit
Frutas	Joker Crypter	NakedBind
FTW Logger	JPS	nBinder
G-Pack	Jrat	Nessus
GhonZilla	KBW Logger	NetDevil
Gids KeyLogger	kCrypter 1.0	NetOris v3.0.3
Gio Crypter	KeyCopy	Network Stresser
Golden Phoenix RAT	KeySpy	NewHacks Crypter
Good Bye	kick21 Crypter	Nikto2
Graeme	Kismet	Nmap
GraphicBooting RAT	KobacCrypter	Nova Crypter Server
Grieve Crypter	L0phtCrack	NovaLite
H-Keylogger	L33T Decrypter	Nstealth HTTP
H4k3r.69.91's Dark Logger	l3v3l-23	NT Packer
Hackers Utility	Lab Stealer	Nuclear RAT
Hallow's Scantime Crypter	Legion NetBios Scanner	nufcrule3 Crypter
Halloween Crypter	LethalLogic Keylogger	Nytro RAT
Hatrex Crypter	Limitless	Octrix Crypter
Havij	Limitless Logger	Oh year Crypter
HC Stealer	LogikLogger	Optix
Heaven Crypter	LokiRAT	P0f
Icepack Platinum	Lord PS	p0ke's WormGen
iEncrypt	Lost Door	PaiN RAT
Illusion Crypter	Luiz Eleonore	Pak EyE Crypter
Infinity Crypter	Metasploit	Panther Mode
IPKiller	MeTuS Delphi	Paradox
Iris	MicroCrypter	Paroxproxy.org

(...continued on the next page)

PassStealer	Shell Laps Icon Changer	Titanium Stresser
Phoenix	ShockLaps File Binder	ToThoZ Keylogger
Pocket RAT	Sick Logger	Triloko Crypter
Poison Ivy	Sikandar's Keylogger	Trojan Hunter
Polifemo Ebrio Crypter	SilverLogger	Turkish ARTA
Polymorphic KeyLogger	SimpleStealer	Turkojan
Predator Keylogger	Site Hog	uBinder
Project Neptune	SKL	Ultimate Logger
ProPort	SkuLogger	Unicornscan
ProRAT	Skyneos Keylogger	Unique Pack
Protector	Smart Pack	University1337
pwdump6	SmartCrypt	Unkown
PWStealer	Smoke Loader	Unlimited PW Stealer
Pytho	SolarWinds	Vaqxination
RainbowCrack	Solitude	VBSwg
Rapid Keylogger	Soul Logger	VoidEye CGI Scanner
RapZo Logger	Special HackHound	Wbrute
RDG Tejon Crypter	Spy-rat	Win-spy
rDoS	SpyEye	Wireshark
RDS	SQLI Helper	WTF Crypter
Ref Stealer	SQLINJ	X-Pack
Reflect Logger	SS-RAT	Xeus
Refruncy Crypter	SSRAT	Xprobe2
Rei Da Rua Crypter	Stealth Crypter	XR Host Booter
Remote Penetration	Stumbler	XSS Scanner
RESIDUO	Stupid Stealer	XtremeRat
Retina	Sub7	XYZ Keylogger
Rocker	SuperScan	Y3 RAT
RPC Nuke	SYN Flood	YAB
Sadaf Keylogger	Target-Exploit	zDoS
Scanarator	TE Port Scanner	Zeus
Schwarze	Tenable Network Security	ZH Stealer
Shark	THC-HYDRA	zoOk Crypter
Sharp-Stealer	The Best Keylogger	
Sheikh Crypter	Themida	

Note: This list only contains the names of crimeware tools that were made available directly for download from a website link or implied to be accessible in a discussion thread in which a website link was provided through a private message (PM). Crimeware “collections” as a single file download are not listed above. For example, if a discussion thread posted a link for a collection of 1000 different crimeware tools in a single file, such names of tools are not listed above.

Appendix 2: Glossary of acronyms and jargon used in discussions

0day - A security hole on a system that is unknown to the owner of the system.

BTC - Abbreviation for "bitcoin". It is a type of cryptocurrency that only exists online or on a computing device.

booter - Same as a "stresser". A tool that performs the function of a "DDoS" attack.

bot - A single computer on the Internet, among many, that are controlled by a cybercriminal.

botnet - Multiple computers on the Internet that are controlled by a cybercriminal.

cpanel - Abbreviation for "control panel". A website interface that allows a cybercriminal to control their botnet.

crack - Cracked software is a program that has been circumvented against the wishes of the original creator or distributor.

crypter - A tool that hides malicious software from being detected by its target.

DDoS - Acronym for "distributed denial of service". A cyberattack where multiple computers (or a single system) overwhelms a target with Internet traffic.

dork - Involves the technique of using searches, typically on Google, to identify websites that have security vulnerabilities.

dox - Involves the collection and release of personal information of a victim.

exploit - An "exploit kit" (software tool) or "exploit code" (snippet of code) that aims to take advantage of a security vulnerability or exploit.

FUD - Acronym for "full undetectable". An adjective used to describe a malicious file, or a **crypter**, that cannot be detected by anti-malware products.

HTTP bot - A botnet, which is controlled by a cybercriminal, that uses the HTTP "website" protocol to communicate.

i4i - Abbreviation for "install for install". The trading of access to botnets between cybercriminals.

IRC bot - A botnet, which is controlled by a cybercriminal, that uses chatroom servers to communicate.

JDB - Abbreviation for "java drive-by". A technique used by cybercriminals that tricks a user into downloading a malicious Java file.

LR - Abbreviation for "Liberty Reserve". A service that allows people to transfer money.

Monetize – Establish ways to make money. In the cybercrime scenario, this can involve online fraud through the use of crimeware.

Phishing – Technique used by cybercriminals to trick victims into revealing personal information such as a login id, password, and financial information.

PM - Abbreviation for "private message".

port - A communication channel on a computer. A secondary meaning, more specifically *porting*, involves the transfer of control from one botnet family to another botnet family.

port forward - A typical Internet connection includes a computer that is connected to a gateway such as a WiFi router that is connected to the Internet. Traffic can be redirected at the gateway level and forwarded to a specific program on the computer.

proxy - A computer that acts as an intermediary and forwards traffic. Examples include a bot or VPS.

RAT - Abbreviation for "remote access trojan".

sandbox - A technique used by security researchers (as well as hackers and cybercriminals) to keep isolated malicious files from causing unwanted actions on their computer.

scanner - Also referred to as a "web scanner". It is a feature of a tool that scans for potential security holes on a system connected to the Internet.

shell - A simple program that allows a cybercriminal to manipulate files on a compromised computer or server.

SQL - In the case of cybercrime, it refers to "SQL injection" which is a technique used by cybercriminals to "break into" a website.

SSH – Acronym for “secure shell”. It is a protocol used to encrypt remote events. For example, if a user logs in remotely, the login id and password would be encrypted, preventing the likelihood of “eavesdropping” by a third party.

stealer - Similar in function to a keylogger. It may also be referred to as a “form grabber”.

stresser - Same as a "booter". A tool that performs the actions of a "DDoS" attack.

VPN - Abbreviation for "virtual private network". Provides remote access to a system that is also encrypted, which prevents the likelihood of “eavesdropping" by a third party.

VPS - Abbreviation for "virtual private server". Its function is similar to that of a "bot" when used as a “proxy”, except that access is typically provided as a legitimate service.

WU - Abbreviation for "Western Union". A service that allows people to transfer money.

XSS - Abbreviation for "cross-site scripting". It is a type of security vulnerability that is taken advantage by a cybercriminal to capture activity on a victim's web browser.

Appendix 3: Additional details on methodology

The goal of this section is to supplement Chapter 3 that explains the collection and analysis of the web forum site data. Certain details were purposefully omitted from Chapter 3 for the reason that it was not essential to explain the findings, however they may assist in validating the methodology (for researchers seeking to replicate the study). Moreover, an attempt was made to condense the explanation of the methodology, as it was presented in Chapter 3. To readers well versed in methodological approaches of examining non-traditional data such as web forum sites (e.g., data that does not involve face-to-face interviews, surveys or crime statistics), Chapter 3 will certainly appear to be missing information. The full detailed contents of the analysis (e.g., rough notes, reflexive journal, spreadsheets, open/axial/selective codes, the raw discussion posts) is not provided in this appendix, rather the focus is to explain *particularly unclear points* in the methodological process.

Selection, collection, examination and coding via multiple iterations (web forums sites)

As highlighted in Chapter 3, the first four web forum sites were identified, each through the use of search engines via www.google.com, www.bing.com, www.yahoo.com and www.ask.com, and the next five web forum sites were selected through online polls that were posted on each of the first four web forum sites. Two of the five sites identified from the polls were no longer accessible during the data collection phase of the research, and were thus removed from the study. An additional web forum site was subsequently added that was hosted on Tor, providing a total of eight web forum sites.

To clarify, the actual process of the selection of sites did not occur through a stepwise process, which may be implied. The identification of sites occurred iteratively, and in parallel with the analysis of the web forum site contents. For example, the first site was identified via Google and was subsequently examined. As the first site did not provide enough data for examination, a second site was identified through another search engine and examined. The second site did not yield enough data for analysis, so a third site was added. At each point, themes were identified (via open coding) among the discussion

groups, and it was subsequently identified that some discussion groups were entirely unrelated to crimeware or crimeware-related activities and were thus omitted. Once the discussion groups were coded, the contents of the discussion threads were examined. A fourth site was subsequently identified and examined following the same process, and so on. The process of identifying web forum sites, selection of discussion groups within the web forum sites, and the coding of discussion post content overlapped, and this process occurred repeatedly. As themes emerged, further sites were included (via the use of online polls), and then their discussion groups and discussion threads consequently examined. The process was methodical and the identification of codes/themes were consistent but involved multiple iterations. This iterative process continued over the longest possible time frame (one year) largely guided by time and resource limitations. The largest sample of discussion groups examined numbered 4410, which was subsequently reduced to capture only relevant discussion groups.

An operational element of grounded theory, an iterative process is described as "theoretical sampling" (Chenitz & Swanson, 1986), and is based on grounded theory developed by Glaser and Straus in the 1960s. This approach provides for theoretical sensitivity (Glaser & Strauss, 1967) and was employed to avoid inadvertently restricting the researcher to a particular set of data and/or themes. This iterative process, if continued for a sufficient time and performed methodically, indirectly helps to achieve a certain level of saturation. The obvious disadvantages of this approach are that it is seemingly complex to explain and time consuming.

What is grounded theory used and where was it applied? (web forum sites)

Grounded theory is sometimes used interchangeably with *qualitative research*, which is an inaccurate representation. It involves the generation of theory through the *systematic analysis* of data. In the 1980s, two different schools of thought emerged that stressed different aspects of grounded theory, namely by Strauss and Corbin (1990) and Glaser (1992). Melia (1996) suggests that the two strands may in fact be describing the same theory but expressed in a different way. In spite of the different versions, Charmaz (2006) identifies common features among the variants of grounded theory:

- data is collected and analysed iteratively
- social processes are identified
- inductive generation of categories
- categories are refined through sampling
- categories are integrated
- codes are created without drawing from pre-existing knowledge

In the research, this grounded theory approach was applied at two levels: the first level includes the discussion groups and the second level covers the discussion post contents (which are found *within* the discussion groups). To provide a glimpse into the *theoretical sampling* process of the selection of discussion groups, a sample of the coded data is provided (from one of the earlier iterations).

The chart below (see Table A) reveals the codes (themes) identified at the first level (the discussion groups). Note that a maximum of 4410 discussion threads were collected, which was later decreased to 1450 (these were purposively selected based on identified themes and only included relevant discussion groups) to obtain the sample used in the final analysis. The 4410 discussion threads were coded according to the nature of the group discussion namely, discussion groups that focused on knowledge transfer (for example, tutorials), software/crimeware-specific (for example, tools related to botnets) and transactional exchanges (for example, buyer-seller markets). Note that some discussion groups fell under more than one group/theme. To provide one example, 95 discussion threads were saved from Forum A (A4 in Table A), 50 from the main discussion group and 15 from each of the sub-discussions (50 + 15 + 15 + 15 = 95) – this discussion group focused on software/crimeware.

Table A: Categories (knowledge, software/crimeware-specific, transactional)

Discussion group	Number of sub-discussion groups	Number of discussion threads (factoring in sub-discussions)	Group 1: "Knowledge"	Group 2: "Software / crimeware-specific"	Group 3: "Transactional"
A1	1	65	X		
A2	3	95	X		
A3	2	80	X		

A4	3	95		X	
A5	0	50	X	X	
A6	0	50	X		
A7	0	50	X		
A8	0	50	X		
A9	0	50	X	X	
A10	4	110	X		
A11	1	65		X	X
A12	3	95			X
A13	3	95			X
A14	1	65		X	
A15	0	50	X		
B1	0	50		X	
C1	0	50	X	X	X
C2	0	50	X		X
C3	1	65	X	X	
C4	1	65	X		
C5	2	80	X	X	
C6	1	65		X	
C7	0	50		X	
C8	2	80	X	X	X
C9	0	50		X	
C10	1	65	X	X	
C11	0	50	X	X	
C12	0	50	X	X	
C13	0	50	X	X	
C14	0	50		X	X
C15	0	50		X	X
C16	0	50		X	X
C17	0	50		X	X
C18	0	50			X
C19	3	95			X
C20	0	50		X	X
C21	1	65	X		
D1	0	50	X	X	X
D2	1	65	X	X	X
D3	1	65	X	X	
D4	0	50	X		
D5	0	50			X
D6	0	50			X
D7	0	50			X
E1	2	80	X		
E2	1	65		X	
E3	0	50	X		
E4	0	50		X	

E5	0	50	X		
E6	3	95		X	
E7	0	50	X	X	
E8	0	50		X	
E9	0	50		X	
E10	0	50		X	
E11	0	50		X	X
E12	0	50			X
F1	0	50	X	X	
F2	0	50	X		
F3	0	50		X	
F4	0	50	X		
F5	2	80		X	X
F6	0	50		X	X
F7	0	50	X		
F8	0	50		X	X
G1	0	50	X		
G2	0	50		X	
G3	1	65	X		
H1	0	50	X		
H2	0	50	X		
H3	0	50	X	X	
H4	0	50		X	
H5	0	50	X	X	
H6	0	50	X	X	
H7	0	50	X	X	
H8	0	50			X
Total		4410			

The chart below (see Table B) reveals the themes identified from the discussion groups in a later iteration (using different codes), which produced a sample that was too small.

Table B: Categories (nature of discussion group)

Nature of discussion group	Discussion group					
remote access trojans	C9	D3	E8			
general tools	A4	B1	H4	C6	E4	
bots and botnets	A9	D3	E5	E6	F4	H5
exploits and exploit code	C3	H7				
crypters	E8	C7	A8			
loggers	C11	E10				
tutorial	A2	C4	D4	E3	H2	
beginners, new members	A1	D1	H1			
monetisation (ways to make money)	A15	E1				
"website" focused hacking	A3	C5	H3			

***A priori* codes from "learning"**

Being true to grounded theory, past beliefs, preconceptions or expectations should be precluded when examining data. An alternative approach to coding involves the use of *a priori* codes (Taylor & Gibbs, 2010). These are simply codes that are determined based on pre-existing purposefully selected theories. As Dey (1999) put it, "there is a difference between an open mind and an empty head" (p. 251). The coding applied at the first level (discussion groups) was true to grounded theory, as it did not involve applying any pre-existing schemes. However, the coding applied at the second level (discussion post contents) employed the *a priori* approach drawing from Soller's (2001) collaborative social learning skills taxonomy (CSLST). The researcher considers the use of *a priori* to fall under *grounded theory*, but an extension of the original conception summarised in this appendix by Charmaz (2006). Refer to Table 2 in Chapter 3.4 on the *a priori* codes that were used - the codes under "New themes" are themes that are not found in the original CSLST, which were added to describe additional characteristics of the data. As a student of criminology that has been influenced by past models on "learning theories", it made sense to acknowledge this bias outright via the use of *a priori* codes.

How did the open, axial and selective coding process take place? (web forum sites)

To briefly describe the coding process in qualitative research, open coding is concerned with identifying and labelling patterns, axial coding is the process of linking codes typically focusing on causal relationships, and selective coding is similar to axial coding except certain codes are purposefully selected and other codes are related to those selected codes.

In the thesis, the open codes relied on CSLST that were used as *a priori* codes, in addition to the newly generated codes listed under "New themes" in Table 2 in Chapter 3.4.

The axial codes include the various relationships between the open codes. A few of these are noted along with examples:

- seller - exchange (monetary) - tool (crypter) => “member selling their crypter”
- encourage - innovation => “member seeking assistance to develop a tool”
- target other member - deception => “member has downloaded a tool that infected them”
- request information - helpfulness => “member receives a useful response about a question”

The selective codes are the themes identified that correspond to the sections in the main data chapters (Chapter 4 and 5) namely, new users, basic elements of learning, learning contributors, learning detractors, existence of social structures, attributes, innovation, intention, motivation, targeting, and value.

Appendix 4: Interview information (Participant Information Sheet)

Participant Information Sheet

Researcher:

My name is Ki Hong (Steve) Chon and I am a PhD student from the Australian National University. I am a student in the Centre for Arts and Social Science at the university. I also work as a part-time casual Research Assistant working on a project related to monitoring crime on the Internet.

Project Title: Crimeware, Online Communities and Cybercrime

General Outline of the Project:

Description and Methodology: The goal of this project is to gain a greater understanding of the market for tool kits and related services to examine implications in relation to regulation and policy. Tool kits consist of a type of malicious software designed to carry out or facilitate illegal online activity, known as crime, and is often associated with hacking and online fraud activities. These particular tools are used by a wide range of people from IT security professionals to "black hat" hackers with malicious intentions and we wish to canvass as many current and potential users as possible. Please note that the first phase of the project involved an observation study focused on examining online discussion forums involved in various crimeware activities – the goal was to identify trends, patterns and themes among the population observed. The second phase of the research involves interviews, with individuals such as your self, to provide context and insight into the activities in the forums.

Participants: Interviews with key stakeholders such as computer security professionals, public sector Internet first responders including law enforcement, and offenders will be undertaken who are involved in monitoring or has had sufficient interaction with crimeware. Please note that the interviews that I am seeking from you will be used in the second phase of the research project.

Use of Data and Feedback: The data will be presented in the form of an 80,000+ word academic publication, as well as two or three 10,000 word academic journal publications. In the event any information that you provide is used in any publication, a copy of the publication will be provided to you prior to publication and after publication.

Project Funding: This study is funded by an Australian Research Council Discovery Projects grant (see http://www.arc.gov.au/discovery-projects). Funding is not connected to any governmental or law enforcement agency.

Participant Involvement:

- **Voluntary Participation & Withdrawal**: Participation in the interview is voluntary**.** There are no negative consequences if you decline to take part or withdraw from the research at any time. You may refuse to answer a question. If you decide to withdraw, all data provided by yourself will be permanently deleted.

- **What does participation in the research request of you?** The interview will be open-ended, although guided by the topic on what you know or have experience with in relation to crimeware, botnets and hacking activities. You may choose to have the interview recorded over audio. If recording is not an option, the researcher will make notes on paper during or immediately after the interview based on your preference.

Australian National University

- **Location and Duration:** The interviews will take place in any area you choose. The duration should be between 30 minutes up to 2 hours. There are no time limits. You may terminate your participation at any time during the interview.

- **Remuneration:** No remuneration will be provided.

- **Risks:** If in the event you inadvertently reveal information that you did not intend to reveal, this information will not be used, saved or referred to in the research.

- **Benefits:** The research will contribute to the development of strategies to reduce risks and to better understand illicit behaviour related to crimeware. The research also seeks to identify problems with current government and industry policies, and explore the ethical boundaries of using tool kits (crimeware) and related services.

Confidentiality:

Confidentiality: Confidentiality will be protected as far as the law allows. All information and responses provided to us will remain anonymous in relation to this study. Individual information collected will not be released to any governments or law enforcement agencies. Any references to individuals, groups or organizations will be anonymized and coded to prevent identification when reported in publications. The pursuit of this research is purely for academic purposes.

Data Storage:

- **Where:** The data will be stored in a secured (secret) location on campus at the Australian National University.

- **How long:** All data will be destroyed no longer than 1 year after publication of the 80,000 word research project in 2015.

- **Destruction of Data:** The hard drives used to store the data will be destroyed permanently using magnets to ensure the data cannot be recovered. Electronic data destruction will be destroyed in such a manner that it is impossible to recover. Any data noted on paper will be destroyed properly using a shredder and disposed of securely.

Queries and Concerns:

- **Contact Details for More Information:**
  Ki Hong (Steve) Chon, Tel: +61 2 612 56043, Email: Steve.Chon@anu.edu.au
  Professor Roderic Broadhurst, Tel: +61 2 612 54665, Email: Roderic.Broadhurst@anu.edu.au

Ethics Committee Clearance:

The ethical aspects of this research have been approved by the ANU Human Research Ethics Committee. If you have any concerns or complaints about how this research has been conducted, please contact:

Ethics Manager
The ANU Human Research Ethics Committee
The Australian National University
Telephone: +61 2 6125 3427
Email: Human.Ethics.Officer@anu.edu.au

References

Abadinsky, H. (2007). *Organized crime*. Nelson Education.

Ackland, R. (2013). *Web social science: Concepts, data and tools for social scientists in the digital age*. Sage.

Adams, B. N., & Sydie, R. A. (2001). *Sociological theory*. SAGE Publications.

Akers, R. L. (1977). *Deviant behavior: A social learning approach* (2nd ed.). Belmont, CA: Wadsworth Pub. Co.

Akers, R. L. (2011). *Social learning and social structure: A general theory of crime and deviance*. Transaction Publishers.

Akers, R. L., & Jensen, G. F. (Eds.). (2011). *Social learning theory and the explanation of crime* (Vol. 1). Transaction Publishers.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review*, 636-655.

Alazab, M., & Broadhurst, R. (2014). Spam and Criminal Activity. *Trends and Issues (Australian Institute of Criminology) Forthcoming*.

Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013, November). Malicious spam emails developments and authorship attribution. In *Cybercrime and Trustworthy Computing Workshop (CTC), 2013 Fourth* (pp. 58-68). IEEE.

Andersen, R. (2007, December 31). Hacking tool guidance finally appears. Retrieved from https://www.lightbluetouchpaper.org/2007/12/31/hacking-tool-guidance-finally-appears/

Andersen, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer Berlin Heidelberg.

Australian Federal Police. (2013, September 15). *High tech crime*. Retrieved from http://www.afp.gov.au/policing/cybercrime/hightech-crime

Australian Institute of Criminology. (2007, June). *Money Mules.* High tech crime brief no. 16. Australian Institute of Criminology.

Ayling, J. (2009). Criminal organizations and resilience. *International Journal of Law, Crime and Justice*, *37*(4), 182-196.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, *4*(1&2).

Bailey, K. D. (2001). Systems theory. In *Handbook of sociological theory* (pp. 379-401). Springer US.

Bandura, A. (1977). Social learning theory.

Barak, G. (1998). *Integrating criminologies*. Boston: Allyn and Bacon.

Barford, P., & Yegneswaran, V. (2007). An inside look at botnets. In *Malware Detection* (pp. 171-191). Springer US.

Bartollas, C. (2005). *Juvenile delinquency* (7th ed.). Boston: Allyn & Bacon.

Beccaria, C. (1764). *On crimes and punishments*.

Bentham, J. (1891). *A fragment on government*. The Lawbook Exchange, Ltd.

Berg, B. L., & Lune, H. (2004). Qualitative research methods for the social sciences (Vol. 5). Boston: Pearson.

Berka, J. (2007, July 30). *Lead developer of KisMAC calls it quits*. Retrieved from http://arstechnica.com/apple/2007/07/lead-developer-of-kismac-calls-it-quits/

Bertalanffy, L. V. (1968). *General system theory: Foundations, development, applications* (p. XV). New York: Braziller.

Bhattacharjee, Y. (2011, January 31). *How a remote town in Romania has become cybercrime central*. Retrieved from http://www.wired.com/2011/01/ff_hackerville_romania/

Bisson, D. (2014, December 16). *FBI Used Metasploit Hacking Tool in 'Operation Torpedo'*. Retrieved from http://www.tripwire.com/state-of-security/latest-security-news/fbi-used-metasploit-hacking-tool-in-operation-torpedo/

Black, D. (1976). *The behavior of law*. New York: Academic Press.

Blunden, B., & Cheung, V. (2014). *Behold a pale farce: Cyberwar, threat inflation, & the malware industrial complex*. Trine Day.

Bowers, K. J., & Johnson, S. D. (2003). Measuring the geographical displacement and diffusion of benefit effects of crime prevention activity. *Journal of Quantitative Criminology*, *19*(3), 275-301.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Sage.

Brantingham, P., & Brantingham, P. (2008). 5. Crime pattern theory. *Environmental criminology and crime analysis*, 78.

Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *NCJL & Tech.*, *4*(1).

Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. ABC-CLIO.

Brenner, S. W. (2014). *Cyberthreats and the Decline of the Nation-state*. Routledge.

Brenner, S. W., & Clarke, L. L. (2004). Distributed security: Preventing cybercrime. *J. Marshall J. Computer & Info. L.*, *23*, 659.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: trends and challenges. In Handbook of Asian criminology (pp. 49-63). Springer New York.

Broadhurst, R., & Choo, K. K. R. (2011). Cybercrime and online safety in cyberspace. *Routledge Handbook of Criminology*, 153.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2013). Organizations and Cybercrime.

Brown, M. (2011, June 27). *LulzSec announces retirement after 50 days of hacking*. Retrieved from http://www.wired.co.uk/news/archive/2011-06/27/lulzsec-retires

Browne, K. (2011). *An Introduction to Sociology.* Polity Press: Cambridge, UK.

Buckley, W. (1967). Sociology and modern systems theory.

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behaviour. *Social problems*, 14(2), 128-147.

CB Insights. (2013, September 3). *As threats increase, cybersecurity software and hardware sees uptick in VC deals and funding – $1.4 billion across 239 deals in last year.* Retrieved October 8, 2014, from https://www.cbinsights.com/blog/cybesecurity-venture-capital/

Center for Problem-Oriented Policing. (n.d.). 25 Techniques of Situational Prevention. Retrieved from http://www.popcenter.org/25techniques/

CERT Australia. (2012). *Cyber crime & security report 2012.* Retrieved from https://www.cert.gov.au/system/files/614/679/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf

Chabinsky, S. R. (2010, March 23). *The cyber threat: Who's doing what to whom?* FBI. Retrieved from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to- whom

Chang, Y. C. (2012). *Cybercrime in the greater China region: Regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing.

Chantler, A. N. (1995). *Risk: The profile of the computer hacker* (Doctoral dissertation, Curtin University of Technology).

Chantler, A. N., & Broadhurst, R. (2006). *Social engineering and crime prevention in cyberspace.*

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis (Introducing Qualitative Methods Series).

Chatziioannou, K. (n.d.). The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data. *Values and Freedoms in Modern Information Law and Ethics*.

Chenitz, W. C., & Swanson, J. M. (1986). Qualitative research using grounded theory. *From practice to grounded theory: Qualitative research in nursing*, 3-15.

Children's Online Privacy Act (COPPA). Retrieved from https://www.law.cornell.edu/uscode/text/47/231

Choo, K. K. R. (2007). *Zombies and botnets*. Australian Institute of Criminology.

Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organized Crime*, *11*(3), 270-295.

Choo, K. K. R. (2011, February). Cyber threat landscape faced by financial and insurance industry. *Trends & Issues in Crime and Criminal Justice*, (408), 1.

Choo, K. K. R. (2011a). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On Line*.

Clarke, R. V. (1992). Successful Case Studies. *Albany, NY: Harrow and Heston*.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 91-150.

Clarke, R. V. (Ed.). (1997). *Situational crime prevention* (pp. 53-70). Monsey, NY: Criminal Justice Press.

Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what?. *Crime Science*, *1*(1), 1.

Cloward, R. (1959, April). Illegitimate means, anomie, and deviant behavior. *American Sociological Review*, 24(2), 164-176.

Cloward, R., & Ohlin, L. (1994). Differential Opportunity and Delinquent Subcultures.

Cloward, R., & Ohlin, L. (2013). Delinquency and Opportunity: A Study of Delinquent Gangs. Routledge.

Cohen, A. K. (1971). Delinquent Boys: The Culture of a Gang.

Cohen, S. (2002). Folk devils and moral panics: The creation of the mods and rockers. Psychology Press.

Cohen, L. E., & Felson, M. (1979, August). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Cohen, L. E., & Felson, M. (2003). *A routine activity approach*. Crime: Critical Concepts in Sociology, 1, 316.

Cohen, A. K., & Short, J. F. (1958). *Research in Delinquent Subcultures*. Journal of Social Issues, 14(3), 20-37.

Coleman, G. (2009). *Code is speech: Legal tinkering, expertise, and protest among free and open source software developers*. Cultural Anthropology, 24(3), 420-454.

Colton, C. C. (1820). *Lacon*. Printed by J. McGowan.

Commentary on Sections. Serious Crime Act 2015 (UK). Retrieved from http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/1 and http://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/2

Computer Misuse Act 1990, Section 3A (UK). Retrieved from http://www.legislation.gov.uk/ukpga/1990/18/section/3A

Convention on Cybercrime. (2001, November). *Council of Europe*. Budapest: Council of Europe.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, *3*, 151-196.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*, 933.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41-96.

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

Corrons, L. (2010, March 3). Mariposa botnet. *Panda Security*. Retrieved from http://www.pandasecurity.com/mediacenter/malware/mariposa-botnet/

Cressey, D. R. (1960). Epidemiology and individual conduct: A case from criminology. *Pacific Sociological Review*, 47-58.

Criminal Code Act 1995 (Australia). Retrieved from https://www.comlaw.gov.au/Series/C2004A04868

Criminal Code (China), 7th ammendment, Art 285, para. 2,3. Translated from Chinese to English by Sergeant Da Chen, Cybercrime Diviosn, Ministry of Public Security (China).

Criminal Code (Germany), cl. 202c. Retrieved from http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html. Translated from German by Prof. Dr. Michael Bohlander at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1754.

Criminal Code (Japan), amended in 2011, Art. 168-2. Translated by Assoc. Prof. Kazutoshi Sugimoto at http://www.waseda.jp/hiken/en/jalaw_inf/topics2011/005sugimoto.html

Criminal Code (Ukraine), Art. 361-1. Retrieved from http://www.legislationline.org/documents/action/popup/id/16257/preview

Cropley, A., & Cropley, D. (2011). Creativity and lawbreaking. *Creativity Research Journal*, *23*(4), 313-320.

Damballa. (2011). *Damballa Threat Report – First Half 2011*. Retrieved from https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf

De Wever, B., Schellens, T., Valcke, M., & Van Keer, H. (2006). Content analysis schemes to analyze transcripts of online asynchronous discussion groups: A review. *Computers & Education*, *46*(1), 6-28.

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175.

Denney, A. S., & Tewksbury, R. (2013). Characteristics of successful personal ads in a BDSM on-line community. *Deviant Behavior*, *34*(2), 153-168.

Denning, D. E. (1996). Concerning hackers who break into computer systems. *High noon on the electronic frontier: Conceptual issues in cyberspace*, *137164*.

Dey, I. (1999). *Grounding grounded theory: Guidelines for qualitative inquiry*. Academic Press.

Diamond, J. (1995, August 1). "Easter's End". *Discover Magazine*. Retrieved from http://discovermagazine.com/1995/aug/eastersend543

Digital Millennium Copyright Act (DMCA). Retrieved from the Library of Congress website: https://www.congress.gov/bill/105th-congress/house-bill/2281

DiMarco, H. (2003). The electronic cloak: Secret sexual deviance in cybersociety. *Dot. cons: Crime, Deviance and Identity on the Internet, Willan Publishing, London*, 53-67.

Donohue, B. (2013, October 21). The Big Four Banking Trojans. *Kaspersky Lab Daily*. Retrieved from https://blog.kaspersky.com/the-big-four-banking-trojans/2956/

D'Ovidio, R., Mitman, T., El-Burki, I. J., & Shumar, W. (2009). Adult-child sex advocacy websites as social learning environments: a content analysis. *International Journal of Cyber Criminology*, *3*(1), 421-440.

Downes, D. M., & Rock, P. (2011). *Understanding deviance: a guide to the sociology of crime and rule-breaking*. Oxford, UK: Oxford University Press.

Doyle, A. C. (1998). *The hound of the Baskervilles*. Oxford, UK: Oxford University Press.

Durkheim, E. (1893). *De La Division Du Travail Social*. Presses Universitaires de France.

Durkheim, E. (1897). *Le suicide: étude de sociologie*. F. Alcan.

Durkheim, E. (1933). *The Division of Labor in Society*. New York: The Free Press.

Durkheim, E. (2013). *Durkheim: The rules of sociological method: And selected texts on sociology and its method*. London: Palgrave Macmillan.

Durkin, K. F. (2007). Show me the money: Cybershrews and on-line money masochists. *Deviant behavior*, *28*(4), 355-378.

Eck, J. E. (1993, September). The threat of crime displacement. In *Criminal Justice Abstracts*, 25(3), pp. 527-546. Retrieved from http://www.popcenter.org/library/psq/1993/Summer_1993_Vol_6_No_3.pdf

Ekblom, P. (n.d.). Conjunction of Criminal Opportunity. Retrieved from https://5isframework.files.wordpress.com/2013/12/cco-for-5is-site.doc

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk Security and Crime Prevention*, *2*, 249-266.

Ekblom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles?. *Studies on Crime and Crime Prevention*, *8*, 27-51.

Ekblom, P. (2001). The conjunction of criminal opportunity: A framework for crime reduction toolkits. *Policing and Reducing Crime Unit Research, Development and Statistics Directorate.* Retrieved from http://r.deception.org.uk/sites/default/files/research/Ekblom_Framework_Reduction_2001.pdf

Ekblom, P. (2005). The 5Is framework: Sharing good practice in crime prevention. *Quality in Crime Prevention*, 55-84.

Ekblom, P. (2012). How to police the future: scanning for scientific technological innovations which generate potential threats and opportunities in crime, policing and crime reduction. In M.J. Smith & N. Tilley (Eds.), *Crime science* (pp. 27-55). New York, NY: Routledge.

Ekblom, P. (2014). Designing products against crime. In *Encyclopedia of Criminology and Criminal Justice* (pp. 948-957). Springer New York.

Ekblom, P., & Gill, M. (2015). Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime. *European Journal on Criminal Policy and Research*, 1-21.

Ekblom, P., & Tilley, N. (2000). Going equipped. *British Journal of Criminology*, *40*(3), 376-398.

Elazari, K. (2014, March). *Hacker's the Internet's immune system*. Retrieved from https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system?language=en

Electronic Frontier Foundation. (n.d.). Digital Millenium Copyright Act. Retrieved October 18, 2015, from https://www.eff.org/issues/dmca

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Official Journal of the European Union. L218/8. Retrieved from http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF

FBI. (2014, May 19). *International blackshades malware takedown*. Retrieved from https://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown

Federal Weapons Act 1972 (Germany). Retrieved from http://www.gesetze-im-internet.de/englisch_waffg/englisch_waffg.html

Felson, M. (1986). Linking criminal choices, routine activities, informal control, and criminal outcomes. In *The Reasoning Criminal* (pp. 119-128). Springer New York.

Felson, M., & Clarke, R. V. G. (1998). *Opportunity makes the thief: Practical theory for crime prevention* (Vol. 98). London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007, October). An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM Conference on Computer and Communications Security* (pp. 375-388).

Furnell, S. (2010). Hackers, viruses and malicious software. *Handbook of Internet Crime*, 173-193.

Gambetta, D. (1996). *The Sicilian Mafia: the business of private protection*. Cambridge, MA: Harvard University Press.

Gambetta, D. (2009). *Codes of the underworld: How criminals communicate*. Princeton, NJ: Princeton University Press.

Gibson, W. (1990). Neuromancer. New York, NY: Penguin Group.

Gill, M. (2005). Reducing the capacity to offend: Restricting resources for offending. *Handbook of Crime Prevention and Community Safety*, 306-328.

Glaser, B. G. (1992). *Emergence vs forcing: Basics of grounded theory analysis*. Sociology Press.

Glaser, B., & Strauss, A. (1967). The discovery ofgrounded theory. *London: Weidenfeld and Nicholson*, *24*(25), 288-304.

Glaser, R., & Bassok, M. (1989). *Learning theory and the study of instruction (Technical Report No. 11)*. Pittsburg, PA: Pittsburgh University PA Learning Research and Development Center.

Glenny, M. (2012). *DarkMarket: How Hackers Became the New Media*. New York, NY: Vintage Books.

Gold, R. L. (1958). Roles in sociological field observations. *Social forces* (36)3, 217-223.

Golding, M. P., & Edmundson, W. A. (Eds.). (2008). *The Blackwell guide to the philosophy of law and legal theory*. Malden, MA: Blawell Publishing

Grabosky, P. N. (1996). Unintended consequences of crime prevention. *Crime prevention studies*, *5*, 25-56.

Grabosky, P. (2001). The Global and Regional Cyber Crime Problem. Proceedings of the Asia Cyber Crime Summit, 22-42.

Grabosky, P. N., Smith, R. G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge, UK: Cambridge University Press.

Green, S. P. (2009). Is There Too Much Criminal Law?. *Ohio State Journal of Criminal Law*, *6*.

Hagan, F. E. (2012). *Introduction to criminology: Theories, methods, and criminal behavior*. Los Angeles, CA: Sage.

Hannemyr, G. (1999). Technology and pleasure: Considering hacking constructive. *First Monday*, *4*(2).

Higgins, G. E., & Makin, D. A. (2004). Does social learning theory condition the effects of low self-control on college students' software piracy. *Journal of Economic Crime Management*, *2*(2), 1-22.

Hilbert, R. A. (1989). Durkheim and Merton on anomie: An unexplored contrast and its derivatives. *Social Problems*, *36*(3), 242-250.

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley: University of California Press.

Hirschi, T. (1986). On the compatibility of rational choice and social control theories of crime. *The reasoning criminal: Rational choice perspectives on offending*, 105-118.

Hirschi, T., & Selvin, H. C. (1967). *Delinquency research: An appraisal of analytic methods* (pp. 106-106). New York: Free Press.

Ho, D. Y. (1998). Interpersonal relationships and relationship dominance: An analysis based on methodological relationism. *Asian Journal of Social Psychology*, *1*(1), 1-16.

Holland, P. C. (1984). Differential effects of reinforcement of an inhibitory feature after serial and simultaneous feature negative discrimination training. Journal of Experimental Psychology: Animal Behavior Processes, 10(4), 461.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. Deviant Behavior, 28(2), 171-198.

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Journal of Criminal Justice Education*, *21*(4), 466-487.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165-177.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, 23(1), 33-50.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891-903.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization*. *Criminology*, *46*(1), 189-220.

Hulme, G. (2012, October 5). *Metasploit Review: Ten Years Later, Are We Any More Secure?*
Retrieved from http://searchsecurity.techtarget.com/feature/Metasploit-Review-Ten-Years-Later-Are-We-Any-More-Secure

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, *25*(6), 528-535.

Hutchings, A. (2013). *Theory and Crime: Does it Compute?*. Griffith University.

Hutchings, A., & Hayes, H. (2008). Routine activity theory and phishing victimisation: who gets caught in the net. *Current Issues Crim. Just.*, *20*, 433.

Internet Live Stats. (2015, October 3). *Internet users by country*. Retrieved from http://www.internetlivestats.com/internet-users-by-country/

Isajiw, W. W. (2013). *Causation and functionalism in sociology*. Routledge.

Jacques, S., & Wright, R. (2010). Dangerous intimacy: Toward a theory of violent victimization in active offender research. *Journal of Criminal Justice Education*, *21*(4), 503-525.

Jaishankar, K. (2008). Space transition theory of cyber crimes. *Crimes of the Internet*, 283-301.

Japanese law on the prohibition of the possession of special lock picking tools. Retrieved September 14, 2015, from http://law.e-gov.go.jp/htmldata/H15/H15HO065.html

Jewkes, Y., & Yar, M. (Eds.). (2010). *Handbook of Internet crime*. Routledge.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Jorna, P., & Hutchings, A. (2012). *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey*. AIC Reports Technical and Background Paper. Australian Institute of Criminology.

Keel, R. (2005, July 14). Rational Choice and Deterrence Theory. Retrieved October 5, 2012, from http://www.umsl.edu/~keelr/200/ratchoc.html

Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. Penn State Press.

Kienzle, D. M., & Elder, M. C. (2003, October). Recent worms: a survey and trends. In *Proceedings of the 2003 ACM workshop on Rapid malcode* (pp. 1-10). New York, NY: ACM.

Klockars, C. (1980). The contemporary crisis of Marxist criminology. *Radical Criminology*, 92-123.

Krebs, B. (2012, November 29). Online Service Offers Bank Robbers for Hire. *KrebsOnSecurity*. Retrieved from http://krebsonsecurity.com/tag/money-mules/

Krebs, B. (2015, July 15). The Darkode Cybercrime Forum, Up Close. *KrebsOnSecurity*. Retrieved from http://krebsonsecurity.com/tag/iserdo/

Kuhn, T. S. (1962). *The structure of scientific revolutions*. University of Chicago press.

Kuhn, T. S. (1977). The essential tension: Selected studies in scientific tradition and change.

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

Lacassagne, A. (1913). *Des transformations du droit pénal et les progrès de la médecine légale de 1810 à 1912*. Lyon: Rey.

Lauritsen, J. L., Laub, J. H., & Sampson, R. J. (1992). Conventional and delinquent activities: Implications for the prevention of violent victimization among adolescents. *Violence and victims*, *7*(2), 91-108.

L'Engle, M. (2010). *A Wrinkle in Time*. New York, NY: Macmillan.

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime*, *17*(4), 231-249.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., & Savage, S. (2011, May). Click trajectories: End-to-end analysis of the spam value chain. In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 431-446). Los Alamitos, CA: IEEE.

Levy, S. (2001). *Hackers: Heroes of the computer revolution* (Vol. 4). New York, NY: Penguin Books.

Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *Security & Privacy, IEEE*, *11*(1), 78-81.

Luhmann, N. (1975). Systemtheorie, Evolutionstheorie und Kommunikationstheorie. In *Soziologische Aufklärung 2* (pp. 193-203). VS Verlag für Sozialwissenschaften.

Luhmann, N., Ziegert, K. A., & Kastner, F. (2004). *Law as a social system*. Oxford, UK: Oxford University Press.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71-94.

Malterud, K. (2001). Qualitative research: standards, challenges, and guidelines. *The lancet*, *358*(9280), 483-488.

Mansfield, S. (2006). *Keeping a critically reflexive research journal*. University of Dundee.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

Matsueda, R. L. (1988). The current state of differential association theory. *Crime & Delinquency*, *34*(3), 277-306.

Matza, D. (1964). *Delinquency and drift*. New Brunswick, NJ: Transaction Publishers.

Maurushat, A. (2013). Discovery and dissemination of discovering security vulnerabilities. In *Disclosure of Security Vulnerabilities* (pp. 21-33). Springer London.

May, K. A. (1991). Interview techniques in qualitative research: Concerns and challenges. *Qualitative nursing research: A contemporary dialogue*, 188-201.

McGuire, M. (2012). *Organised crime in the digital age*. London: John Grieve Centre for Policing and Security.

McManus, M. M., & Aiken, R. M. (1995). Monitoring computer-based collaborative problem solving. *Journal of Artificial Intelligence in Education*.

Meadows, D. H., & Wright, D. (2008). *Thinking in systems: A primer*. White River Junction, VT: Chelsea Green Publishing.

Melia, K. M. (1996). Rediscovering glaser. *Qualitative health research*, *6*(3), 368-378.

Merces, F. (2015, August 5). *The Brazilian underground market.* A Trend Micro Research Paper. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf

Merton, R. K. (1936). The unanticipated consequences of purposive social action. *American Sociological Review*, *1*(6), 894-904.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*(5), 672-682.

Messner, S. F., & Rosenfeld, R. (1994). Crime and the American Dream.

Mill, J. S. (1869). *On liberty*. Longmans, Green, Reader, and Dyer.

Miller, J. G. (1965). Living systems: Basic concepts. *Behavioral science*, *10*(3), 193-237.

Millington, F. H. (1891). *The Housing of the Poor*. London: Cassell & Company.

Mills, A. J., Durepos, G., & Wiebe, E. (Eds.). (2009). *Encyclopedia of case study research* (Vol. 2). Thousand Oaks, CA: Sage.

Minutaglio, B. (1992, August). Buying Time. *Dallas Life Magazine*. Retrieved from http://www.buyersclubdallas.com

Moore, J. A. (1984). Science as a way of knowing—Evolutionary biology. *American Zoologist*, *24*(2), 467-534.

Moore, R. (2010). *Cybercrime: Investigating high-technology computer crime* (2nd ed.). Oxon, UK: Routledge.

Morris, R. G., & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, *32*(1), 1-34.

Morrison, K. (2006). *Marx, Durkheim, Weber: Formations of modern social thought*. London: Sage.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011, November). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 71-80). ACM. New York, NY: ACM.

Moyer, I. (2001). *Criminological theories: Traditional and non-traditional voices and themes*. Thousand Oaks, CA: Sage.

Murphy, J., Elmer-DeWitt, P., & Krance, M. (1983, August 19). Computers: the 414 gang strikes again. *Time.*

Murphy, D. S., & Robinson, M. B. (2008). The Maximizer: Clarifying Merton's theories of anomie and strain. *Theoretical Criminology*, *12*(4), 501-521.

Natarajan, M., Clarke, R. V., & Johnson, B. D. (1995). Telephones as facilitators of drug dealing. *European Journal on Criminal Policy and Research*, *3*(3), 137-153.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. London: Routledge.

Nissenbaum, H. (2001). Securing trust online: wisdom or oxymoron? *Boston University Law Review*, *81*(3), 635-664.

Nonnecke, B., Preece, J., Andrews, D., & Voutour, R. (2004). Online lurkers tell why. *AMCIS 2004 Proceedings*, 321.

Norris, I. N. (2012). *Mitigating the effects of doxing* (Unpublished doctoral dissertation). Utica College: New York.

Ollman, G. (2009). *Exploring the botnet vs. malware relationship.* Retrieved from https://www.damballa.com/downloads/d_pubs/WP%20Many-to-Many%20Botnet%20Relationships%20(2009-05-21).pdf

Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law and Social Change*, *37*(1), 51-97.

Park, R. E., Burgess, E. W., & McKenzie, R. D. (1984). *The city*. University of Chicago Press.

Parsons, T. (1951). *The social system*. England: Routledge & Kegan Paul.

Police and Justice Act 2006. Retrieved from http://www.legislation.gov.uk/ukpga/2006/48/contents

Poulsen, K. (2012). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York, NY: Broadway Paperbacks.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Quinn, J. F., & Forsyth, C. J. (2005). Describing sexual behavior in the era of the Internet: A typology for empirical research. *Deviant Behavior*, *26*(3), 191-207.

Quinney, R. (1970). *The social reality of crime*. New York, NY: Little, Brown & Company.

Radianti, J., Rich, E., & Gonzalez, J. J. (2009, January). Vulnerability black markets: Empirical evidence and scenario simulation. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1-10). IEEE.

RCMP. (n.d.). In Cybercrime: an overview of incidents and issues in Canada. Retrieved from http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm

Reith, C. (1975). *The blind eye of history: A study of the origins of the present police era*. Patterson Smith.

Reppetto, T. A. (1976). Crime prevention and the displacement phenomenon. *Crime & Delinquency*, *22*(2), 166-177.

Resnick, P., Hansen, D., Riedl, J., Terveen, L., & Ackerman, M. (2005, April). Beyond threaded conversation. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems* (pp. 2138-2139). ACM.

Rice, R. (1974). *The business of crime.* Greenwood Press.

Schacter, D. L., Gilbert, D. T., & Wegner, D. M. (2009). *Introducing psychology*. Macmillan.

Schrire, S. (2006). Knowledge building in asynchronous discussion groups: Going beyond quantitative analysis. *Computers & Education*, *46*(1), 49-70

Schlegel, K., & Weisburd, D. (1994). *White-collar crime reconsidered*. UPNE.

Serious Crime Act 2015 (UK). Retrieved from http://www.legislation.gov.uk/ukpga/2015/9/section/42/enacted

Shelden, R. G., Brown, W. B., Miller, K. S., & Fritzler, R. B. (2015). *Crime and criminal justice in American society*. Waveland Press.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, *34*(4), 495-518.

Smith, R. (2010). *Identity theft and fraud. The Handbook of Internet Crime*. Y. Jewkes & M. Jar (Ed.). Devon: Willan, 273-301.

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22-23.

Soller, A. (2001). Supporting social interaction in an intelligent collaborative learning system. *International Journal of Artificial Intelligence in Education (IJAIED)*, *12*, 40-62.

Sommer, P. (2006). Criminalising hacking tools. *Digital Investigation*, *3*(2), 68-72.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2-3), 111-129

Stack Overflow. (n.d.). *What is a bounty? How can I start one?* Retrieved September 5, 2015, from http://stackoverflow.com/help/bounty

Stephenson, N. (1992). *Snow crash*. London: ROC/Penguin.

Sterling, B. (1993). *The hacker crackdown*. London: Penguin.

Sternberg, J. (2012). *Misbehavior in cyber places: The regulation of online conduct in virtual communities on the Internet*. Rowman & Littlefield.

Stoll, C. P. (1989). *The cuckoo's egg: Tracing a spy through the maze of computer espionage*. New York, NY: Pocket Books.

Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2013). The underground economy of fake antivirus software. In *Economics of Information Security and Privacy III* (pp. 55-78). Springer New York.

Strategies for Qualitative Interviews. (2014, October, 5). Retrieved from http://sociology.fas.harvard.edu/files/sociology/files/interview_strategies.pdf?m=1361986682

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Newbury Park, CA: Sage.

Sussman, V. (n.d.). Lost in Kafka Territory. *U.S. News & World Report*. Retrieved from https://w2.eff.org/legal/cases/PGP_Zimmermann/sussman.article

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review*, *5*(1), 1-12.

Sutherland, E. H. (1947). *Edwin Sutherland: On Analyzing Crime*.

Sutherland, E. H. (1956). *The professional thief*. University of Chicago Press.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 664-670.

Symantec. (2010). *Symantec report on attack kits and malicious websites*. Retrieved from http://www.a51.nl/storage/pdf/b_symantec_report_on_attack_kits_and_malicious_websites_21169171_WPen_us.pdf

Tarde, G. (1903). *The laws of imitation*. New York, NY: H. Holt.

Taylor, C., & Gibbs, G. R. (2010). What is Qualitative Data Analysis (QDA)?. *Online QDA Web Site*.

Team Cymru. (2006). Cybercrime: an epidemic. *Queue*, 4(9), 24-35.

Terrorism Act 2000 (UK). Retrieved from http://www.legislation.gov.uk

Thomas, A. (2007, August 14). German anti-hacker lawmakers ban tools of the trade. *The Inquirer*. Retrieved from http://www.theinquirer.net/inquirer/news/1014791/german-anti-hacker-lawmakers-ban-tools-of-the-trade

Thurlow, C., Lengel, L., & Tomic, A. (2004). *Computer mediated communication*. London: Sage.

Trend Micro. (2011). *The crimeware evolution*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-crimeware-evolution.pdf

Trend Micro. (2011a). *1Q 2011 crimeware report*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_1q2011-crimeware.pdf

Turgeman-Goldschmidt, O. (2005). *Hackers' accounts hacking as a social entertainment*. Social Science Computer Review, 23(1), 8-23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2), 382-396.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481), 453-458.

UNICRI. (2013, January 21). *Cyber thread issues and explanations*. Retrieved from http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations

UNODC. (2013). *Comprehensive study on cybercrime*. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNTOC. (2004). United Nations Convention on Transnational Organized Crime. Retrieved from https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

US CERT. (n.d.). *What is phishing?* Retrieved on October 4, 2014, from https://www.us-cert.gov/report-phishing

US DOJ. (2014, May 19). Manhattan U.S. Attorney and FBI Assistant Director-in-charge announce charges in connection with blackshades malicious software that enabled users around the world to secretly and remotely control victims' computers. *US Department of Justice*. Retrieved from http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection

US DOJ. (2015, July 15). Major Computer Hacking Forum Dismantled. *US Department of Justice*. Retrieved from https://www.fbi.gov/pittsburgh/press-releases/2015/major-computer-hacking-forum-dismantled

Van de Bunt, H., Siegel, D., & Zaitch, D. (2014). Social embeddedness of organized crime. In *The Oxford Handbook of Organized Crime* L. Paoli (Ed.) (p.322). New York, NY: Oxford University Press.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.

Van Duyne, P. C., Pheijffer, M., Kuijl, H. G., van Dijk, A. T. H., & Bakker, G. J. (2003). *Financial investigation of crime: A tool of the integral law enforcement approach*. Wolf Legal Publishers.

Vinter, P. (2012, April 2). Computer expert who stole eight million people's personal details for an 'intellectual challenge' jailed for two and half years. *MailOnline*. Retrieved from http://www.dailymail.co.uk/news/article-2124114/Computer-hacker-Edward-Pearson-Lendale-York-stole-million-people-s-personal-details-jailed-half-years.html

Vold, G. B., Bernard, T. J., & Snipes, J. B. (1998). Theoretical Criminology (4th ed.). New York, NY: Oxford University Press.

Von Lampe, K., & Johansen, P. O. (2004). Criminal networks and trust. On the importance of expectations of loyal behaviour in criminal relations. *Organised Crime, Trafficking, Drugs*, 102.

Walker, D. (2014, May 28). *Criminals fuse Zeus, Carberp code for more sinister trojan.* / Retrieved October 15, 2014, from http://www.scmagazine.com/criminals-fuse-zeus-carberp-code-for-more-sinister-trojan/article/348880

Wall, D. (Ed.). (2003). *Crime and the Internet*. New York, NY: Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity Press.

Wall, D. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime 1. *International Review of Law Computers & Technology,* 22(1-2), 45-63.

Wall, D. (2014). Internet mafias? The dis-organisation of crime on the Internet. In *Organized Crime, Corruption and Crime Prevention* (pp. 227-238). Springer International Publishing.

Walsh, A., & Ellis, L. (2006). *Criminology: An interdisciplinary approach*. Thousand Oaks, CA: Sage.

Watts, R., Bessant, J., & Hil, R. (2008). International criminology: a critical introduction. Routledge.

Webber, C. (2014). Hackers and cybercrime. *Shades of Deviance: A Primer on Crime, Deviance and Social Harm*, 95.

Wilson, M. S. (1954). Pioneers in Criminology I--Gabriel Tarde (1843-1904). *J. Crim. L. Criminology & Police Sci.*, *45*, 3.

Wortley, R. K. (1998). A two-stage model of situational crime prevention. *Studies on crime and crime prevention*, *7*(2), 173-188.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal*, *14*(4), 63-82.

Wortley, R., & Mazerolle, L. (Eds.). (2013). *Environmental criminology and crime analysis*. Willan.

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Yar, M. (2005a). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387-399.

Yar, M. (2013). *Cybercrime and society* (2nd ed.). Thousand Oaks, CA: Sage.

Ye, Q., Xu, M., Kiang, M., Wu, W., & Sun, F. (2013). In-depth analysis of the seller reputation and price premium relationship: a comparison between eBay US and TaoBao China. *Journal of Electronic Commerce Research*, *14*(1), 1-10.

Yip, M. (2010). *An investigation into Chinese cybercrime and the underground economy in comparison with the West* (Unpublished doctoral dissertation). University of Southampton: London, UK.

Yip, M. (2011). *An investigation into chinese cybercrime and the applicability of social network analysis*. Retrieved from http://eprints.soton.ac.uk/272351/

Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: a social network approach to understanding cybercrime. Retrieved from http://eprints.soton.ac.uk/343351/

Yip, M., Shadbolt, N., & Webber, C. (2012, June). Structural analysis of online criminal social networks. In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on* (pp. 60-65). IEEE.

Zetter, K. (2013, January 22). *Student expelled for hacking after investigating security hole.* Retrieved May 10, 2013, from http://www.wired.com/2013/01/student-expelled-exposing-flaw/

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, 1-13.

Zollo, M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. *Organization Science*, *13*(3), 339-351.